NASA Contractor Report 163110

RELIABILITY ANALYSIS OF THE F-8 DIGITAL FLY-BY-WIRE SYSTEM

L. D. Brock and H. A. Goodman

Contract NAS4-2571
October 1981

NASA

NASA Contractor Report 163110

RELIABILITY ANALYSIS OF THE F-8 DIGITAL FLY-BY-WIRE SYSTEM

L. D. Brock and H. A. Goodman
The Charles Stark Draper Laboratory, Inc.
Cambridge, Massachusetts

Prepared for
Dryden Flight Research Center
under Contract NAS4-2571

National Aeronautics and
Space Administration

Scientific and Technical
Information Office

1981

CONTENTS

RELIABILITY ANALYSIS OF THE F-8 DIGITAL FLY-BY-WIRE SYSTEM

L.D. Brock and H.A. Goodman

The Charles Stark Draper Laboratory, Inc.

SUMMARY

The NASA F-8 Digital Fly-By-Wire (DFBW) flight-test program is intended to provide the technology for advanced control systems, giving future aircraft enhanced performance and operational capability. A detailed analysis of the experimental system was performed to estimate the probabilities of two significant safety-critical events:

(1) Loss of primary digital flight-control function, causing reversion to the analog bypass system.

(2) Loss of the aircraft due to failure of the electronic flight-control system.

The analysis covers appraisal of risks due to random equipment failures, generic faults in design of the system or its software, and induced failures due to external events. A unique diagrammatic technique was developed which details the combinatorial reliability equations for the entire system, promotes understanding of system failure characteristics, and identifies the most likely failure modes. The technique provides a systematic method of applying basic probability equations and is augmented by a computer program written in a modular fashion that duplicates the structure of these equations.

Results of the analysis indicate that the F-8 DFBW system has a very high reliability when used in typical 1-hour experimental flights, and no single failure can cause a system failure. However, the analysis shows a rapid increase in failure rate as a function of mission time. Therefore, basic design changes would be needed for commercial applications to either increase levels of redundancy or to provide reconfiguration capability to replace failed elements and maintain a more constant failure rate.

SECTION 1

INTRODUCTION

The F-8 Digital Fly-By-Wire (DFBW) flight experiment is a research flight-test program being carried out with NASA to provide the technology for implementation of advanced control systems in future aircraft, permitting greater operational capability and increased performance. The program is being carried out using an F-8 test aircraft.

One of the most critical requirements for a fly-by-wire system is that it be reliable. If an electronic system is to replace the mechanical connections between the pilot's controls and the control surfaces, then it must have a reliability that is equivalent to the mechanical links it is replacing. The primary goal of the design, construction, and testing of the F-8 DFBW system was to ensure that the electronic flight-control system did not cause any decrease in the reliability of the basic aircraft. The effort expended in meeting this goal has paid off in a very successful flight-test program, which has achieved 73 flights to date with no failure of the triplex DFBW system causing reversion to the backup system.

The purpose of the study reported here was to supplement the understanding of the system by performing a detailed reliability analysis. The objective was to predict as accurately as practical the probability that the aircraft will be lost due to a failure of the electronic flight-control system. A further objective was to predict the probability of losing the primary digital control mode, which would cause a reversion to the analog bypass mode.

The outline of the approach taken for the analysis is given in Section 2. The potential hazards are identified first. Then, the flight-control system is analyzed to show the effects of random component failure hazard. The structure created to analyze random failures is then used to identify and evaluate the contributions of other hazards that are more difficult to analyze, such as induced failures and design mistakes.

Section 3 describes the analysis technique developed for random failures, and Section 4 describes the computer program that implements this technique. The development of random-failure rates for the basic system components is given in Section 5, and in Section 6 those component rates are inserted into the system analysis technique to produce a prediction of system unreliability. Section 6 also gives the system failure rate as a function of time and the sensitivity of the system unreliability to the accuracy of the various component failure rates. The results are interpreted to identify the particular failure modes that produce the largest contribution to system unreliability and to investigate system modifications that would reduce that unreliability. Section 7 refines the analysis to allow an evaluation of the effects of factors that were not included in the basic analysis, and expands the analysis for other hazards. Conclusions, observations, and recommendations are given in Section 8.

Appendix A gives a brief history of the F-8 DFBW program. In Appendix B, the F-8 DFBW system is described in sufficient detail to provide a basis for understanding the reliability analysis.

The authors wish to acknowledge the assistance of Ken Szalai of NASA Dryden Flight Research Center (DFRC) for imparting an understanding of the design and operation of the system and for his constructive criticisms on the final draft of this report. We also wish to thank Wilt Lock, also of DFRC, for assisting our understanding of the analog and hydraulic subsystems. Special thanks are also expressed to Vince Megna of The Charles Stark Draper Laboratory, Inc. (CSDL) for his guidance and support as project manager.

This report was prepared by CSDL for NASA under Contract NAS4-2571. Its publication does not constitute approval by NASA of the findings or conclusions contained herein. The report is published for the exchange and stimulation of ideas.

SECTION 2

OUTLINE OF THE APPROACH TAKEN IN THE RELIABILITY ANALYSIS

Study Objectives

The objective of this study was to obtain the best estimates of the probabilities of two separate failure events: the loss of the primary digital flight-control function, and the loss of the aircraft due to a failure of the electronic flight-control equipment. This study emphasizes the second event and computes the probability of the first as a special case within the model that analyzes the complete system.

The guidelines established for this study defined the loss of the aircraft as the complete loss of either pitch control or roll control. Complete loss of pitch control is the loss of both left and right elevators. Complete loss of roll control is loss of both left and right ailerons and loss of the rudder. Loss of control could also be caused by the electronic flight-control system by producing a "hard over" control surface command during a critical time such as takeoff or landing when recovery is not possible.

The analysis in this study is concerned only with probability of aircraft loss due to the failure of equipment added to the aircraft for the experimental program. For example, the primary actuators are not included in the analysis since they are a part of the basic airplane. Original aircraft equipment is included in the analysis only if it interacts strongly with the electronic system. For example, the aircraft hydraulic systems are included in the analysis because hydraulic system failures affect the configuration of the flight-control system and thus the probability of failure.

System Hazards

The objective of this study was to obtain the best estimate of failure by considering all sources of failure that may occur. Many failure modes are well understood and thus easy to analyze, while others are very obscure. The system has been designed to be very tolerant of most well-understood hazards, resulting in a calculated

system failure rate due to these sources in the range of 10^{-7} to 10^{-9} per hour. This very low failure rate greatly increases the significance of the more obscure hazards. It is very difficult, if not impossible, to obtain credible quantitative estimates of the failure rates for many potential failure sources or even to be sure that all significant sources have been identified. The uncertainties of these difficult-to-define sources are large enough compared with the very low failure rates involved that the significance of the failure rates that can be estimated quantitatively is reduced. This study attempts to identify as many sources of failure as practical, while keeping in perspective the significance of the rates that are computed.

The sources of failure considered in this study have been divided into three categories: random equipment failures, specification errors, and induced failures. These failure sources are described briefly in the following subsections.

Random Failures

Random equipment failures include all of the possible failures in the individual system components. These failures are normally caused by the interaction of environmental stress or a particular operational situation with an inherent manufacturing fault in that component or a deterioration in capability after manufacture. These failures are assumed to be random, with little correlation. The rate of failure is determined both by the quality of the original manufacturing, the extent of initial equipment burn-in, and the thoroughness of initial tests, and also by the environmental experience, both accumulated and instantaneous. The statistical failure rate for most of the components that make up the flight-control system are relatively well known from past experience with those, or similar, components and from actual experience with the F-8 system. A discussion of the failures used for this analysis is given in Section 5.

The reliability that can be achieved by individual electronic components normally does not approach the level required for the system. Critical systems are designed to be tolerant of all potential faults in the electronic hardware. When a failure is detected, the system has sufficient additional resources and is able to reconfigure so that the essential functions can continue to be performed. Multiple random failures are thus necessary to cause a failure in a critical flight function. Analysis is necessary to determine the combination of equipment failures that will cause a flight-critical functional failure and the probability of that failure.

Specification Errors

Specification errors include generic faults in the design of the system hardware or software, errors in the manufacturing process itself, and errors in the method specified to operate the system. With redundant channels used to provide coverage for random failures, specification errors can become a dominant source of failure because they can affect all redundant channels simultaneously and cause a complete system failure.

These faults are much more difficult to define, their probability of occurrence is difficult to estimate, and it is not easy to provide protection against them. By definition, there can be almost no actual experience on which to develop an understanding of these failures or estimate their rate of occurrence. This situation can be illustrated by an example. If a particular design is accepted as a standard and is used on all commercial aircraft for a typical generation of 15 years, the total flight time is estimated to be between 10^8 and 10^9 hours. Assuming a required failure rate of 10^{-9} per hour, if there is no failure (or only one) during this time period, it will contribute little to increased understanding and prove little about the statistics. In any case the information would be received too late, as the risk would already have been taken. It is thus necessary to design the system such that it is theoretically close to impossible to have a life-critical failure in the system due to these causes.

It is not claimed that the analysis performed here provides definitive results for these types of faults. The possibility of their existence is recognized. However, an attempt is made to determine their characteristics and to obtain a measure of their relative importance.

Induced Failures

The third category of hazards discussed here are those due to external events. The probability that the flight-control system will continue to provide critical functions after the occurrence of one of these events must be proportional to the probability of that event. The external events considered here are physical damage, fire, lightning, and extreme deviation from the design environment, including temperature, vibration, shock, and electromagnetic interference.

The probability that physical damage and fire will affect the flight-control system can be significant relative to the very low failure

rates that are required. Physical damage can result from collision with other aircraft or birds, collision with the ground or other stationary objects, excessive aerodynamic loads due to abrupt maneuver or turbulence, explosion, massive failure of the engine or other equipment, and loose objects such as tools. Fire can result from many of the same causes as well as massive failure of electrical and electronic equipment, the hydraulic system, etc. Physical damage would also include liquid damage due to fuel, hydraulic, or cargo leaks.

Physical damage is considered the most likely induced failure source for the F-8 aircraft. Lightning would be a significant potential hazard to the system, but is not considered here because flight rules do not allow flights where a potential for lightning exists. Faults could be induced in the system by electromagnetic radiation produced by other equipment external or internal to the aircraft or by the flight-control system itself. The susceptibility of the system to this kind of failure is not easily estimated without a significant amount of testing. Such testing was accomplished on the F-8 DFBW aircraft, but the effects are not considered in this study.

External events can influence the failure rate without directly causing a fault. For example, an environmental extreme such as high heat or vibration can increase the incidence of component failures. This environmental extreme could have happened at some time in the past, but could significantly increase the probability of multiple failures of a particularly sensitive part to a much higher level than would be predicted by random analysis of parts of that generic type.

The Analysis Approach

The analysis approach taken for estimating the probability of loss of the aircraft due to an electronic flight-control system failure was performed in two steps. The first step was to estimate the probability of failure due to random failures of system elements. This constituted a major part of this study. The second step was to refine and extend random-failure analysis to other effects and failure sources.

This approach was taken for several reasons. First, the analytical techniques and the required component failure-rate data is much more readily available for random equipment failures than it is for other types of failure sources. By performing this analysis first, one of the major failure sources can be accounted for, and quantitative estimates can be obtained with a reasonable degree of confidence. These numbers

then serve to establish a baseline for evaluating the importance of the other failure sources. It may not be possible to obtain a quantitative estimate for these other sources, but it may be possible to classify them as either dominant, comparable, or insignificant relative to random failures for which some quantitative estimate is possible.

Performing the analysis for random failures first can provide another advantage. If this analysis is done with the proper forethought, a structure can be created which will aid in the analysis of other failure sources. This structured analysis would allow determination of the interrelationships between failure sources and would indicate the approximate numerical weighting that should be applied to a particular source.

SECTION 3

ANALYSIS OF RANDOM FAILURES

Techniques Considered for Random-Failure Analysis

Several techniques were considered for analyzing random failures, including the classical combinatorial equations and the related fault-tree analysis, Markov analysis, and general-purpose reliability-analysis computer programs. These techniques are discussed in reverse order in the following subsections, which describe the relative advantages and disadvantages of each. This process has led to the development of a graphical technique that facilitates the application of an essentially classical approach.

General-Purpose Reliability-Analysis Programs

Several computer programs have been developed that are intended to aid in estimating system reliability. Three of these, known by the acronyms CAST, CARSRA, and CARE, are described briefly in the following paragraphs.

The first program, the Complementary Analytic-Simulation Technique (CAST),[1]* allows the best features of both analysis and simulation to be used in analyzing system reliability. Analytic modeling can be very flexible and rapid. However, for the more complex systems, the mathematical model can become very involved and almost unmanageable. Simulation can more easily handle system details, but is slow and expensive. These methods are effectively combined in CAST by using an engineering characterization of the computer system to provide input to a fault-driven simulation, which minimizes simulation costs. The simulation produces modeling parameters that are used in the analytic modeling to measure the fault tolerance of the system. This process is shown in Figure 1. Results of applying CAST to typical system configurations is shown in Figure 2.

---

*Superscript numerals refer to similarly numbered items in the list of References.

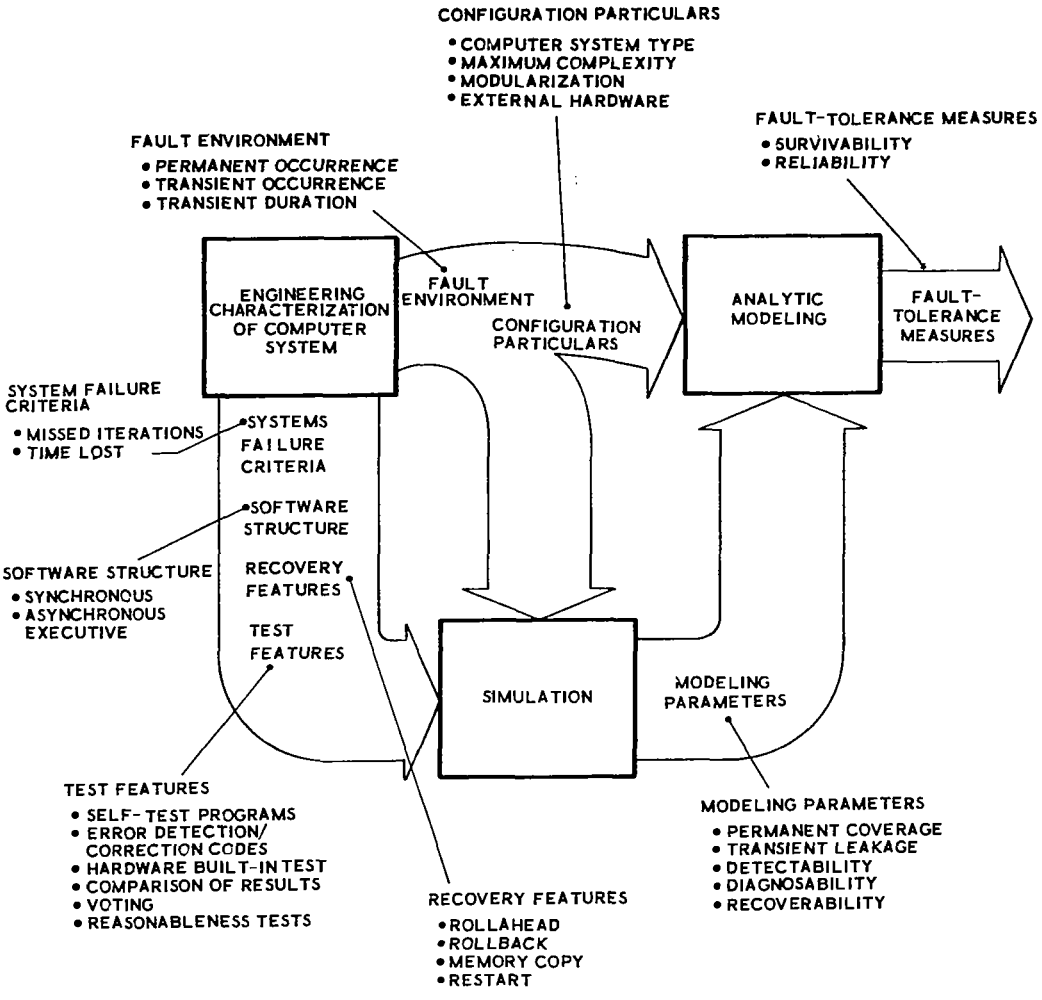


Figure 1. CAST activity sequence and information flow.

The second analysis program is the Computer Aided Redundant System Reliability Analysis (CARSRA).[2] CARSRA is a general-purpose reliability-analysis program that handles modular-redundant reconfigurable systems, taking into account such factors as fault coverage and transient faults. The complexity of a system is overcome by dividing it into stages, where each stage is a set of identical redundant modules. The reliability of each stage is described by a Markov model, and a typical Markov model for a triplex stage is shown in Figure 3, where the potential states are shown for the stage ending in the states of either detected or undetected failure. The symbol λ represents the rate at which a stage transitions from one state to another. For example λ_{12} is the probability that any one module fails in the first stage. An assumption made in this particular model is that there is no transition from state 1 to a failed state. In other words, there is no single-point failure

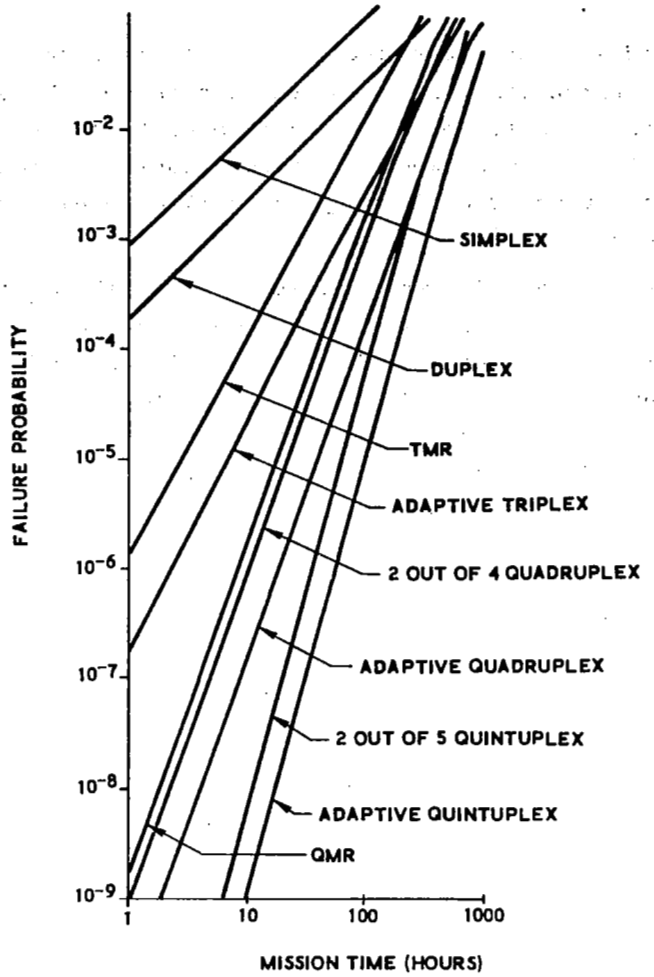


Figure 2. Effects of computer system redundancy and adaptability on failure probability.

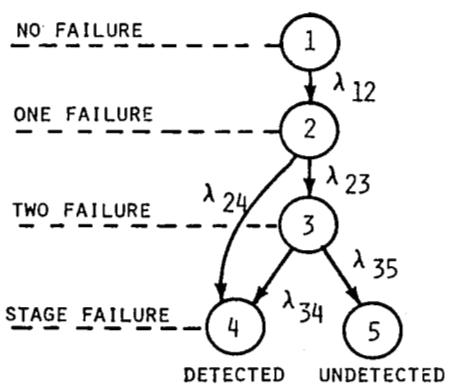


Figure 3. Typical Markov stage model.

mode. This model shows two possible transitions from the one-failure state. In the first case, a second failure causes the stage to fail, and in the other, the stage continues to operate on the one remaining good module. The ratio between these two transition rates is a function of how well the system can identify the failed module by self-test or other techniques.

The Markov models for the individual stages are related by a dependency tree as shown in Figure 4. This dependency tree shows how the failure of a module in one stage will cause the failure of modules in other stages. For example, the failure of a multiplexer and analog-to-digital (A/D) module will cause the loss of one set of modules of all sensor stages that provide information as analog signals. The numbers in each stage are the levels of redundancy. The circles on the right side indicate functional elements needed for the system to survive. The V indicates that voting is used to combine the redundant signals. When the Markov models for each stage, the transition rates, and the dependency are defined as inputs to the CARSRA program, the program computes the functional readiness and failure probabilities for the system.

The third computer program considered is the Computer Aided Reliability Estimation (CARE). CARE refers to a series of programs that have evolved as tools for estimating the reliability of fault-tolerant systems. CARE I was developed at the Jet Propulsion Laboratory,[3] and CARE II was developed for NASA/Langley by Raytheon.[4] CARE III is now under development by Raytheon.[5] The CARE II model is shown in Figure 5.

The system is modeled as a number of "stages", with switchable spares available at each stage. CARE II allows two modes of operation. In mode 1, a defined number of identical units must be functioning at each stage for the system as a whole to be operational. Mode 2 defines another set of numbers for units that must be operating.

The different categories of hardware failures are as follows. Category 3 failures cause system failure even though spares are available, and are thus single-point failures. Category 2 failures cause downgrading to mode 2 even though spares are available for mode 1. Category 1 failures will cause downgrading or system failure if the required spares are exhausted in any particular stage.

The CARE programs handle both permanent and transient failures, and account for recovery from transient failures. These programs also account for imperfect coverage, i.e., the inability to either detect

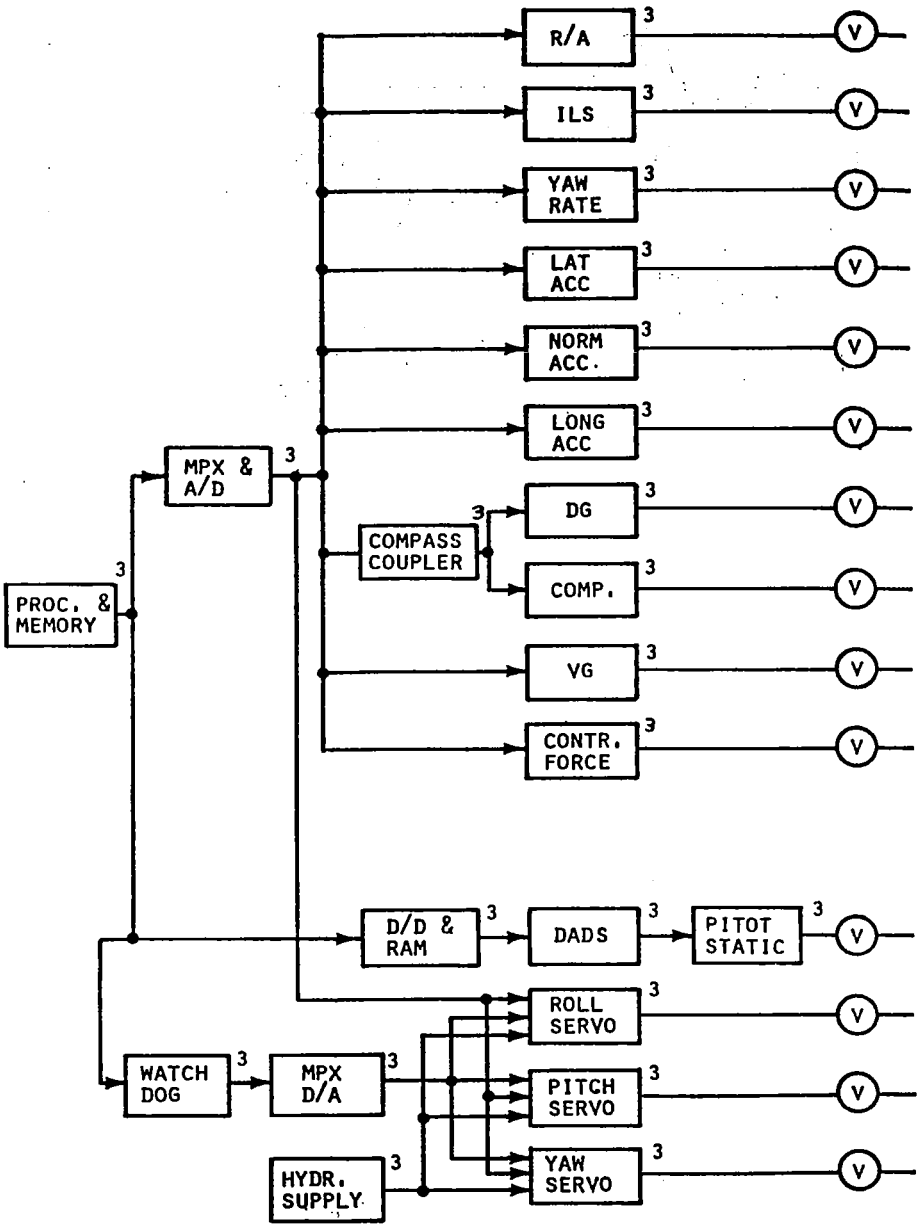


Figure 4. Flight-control system dependency tree.

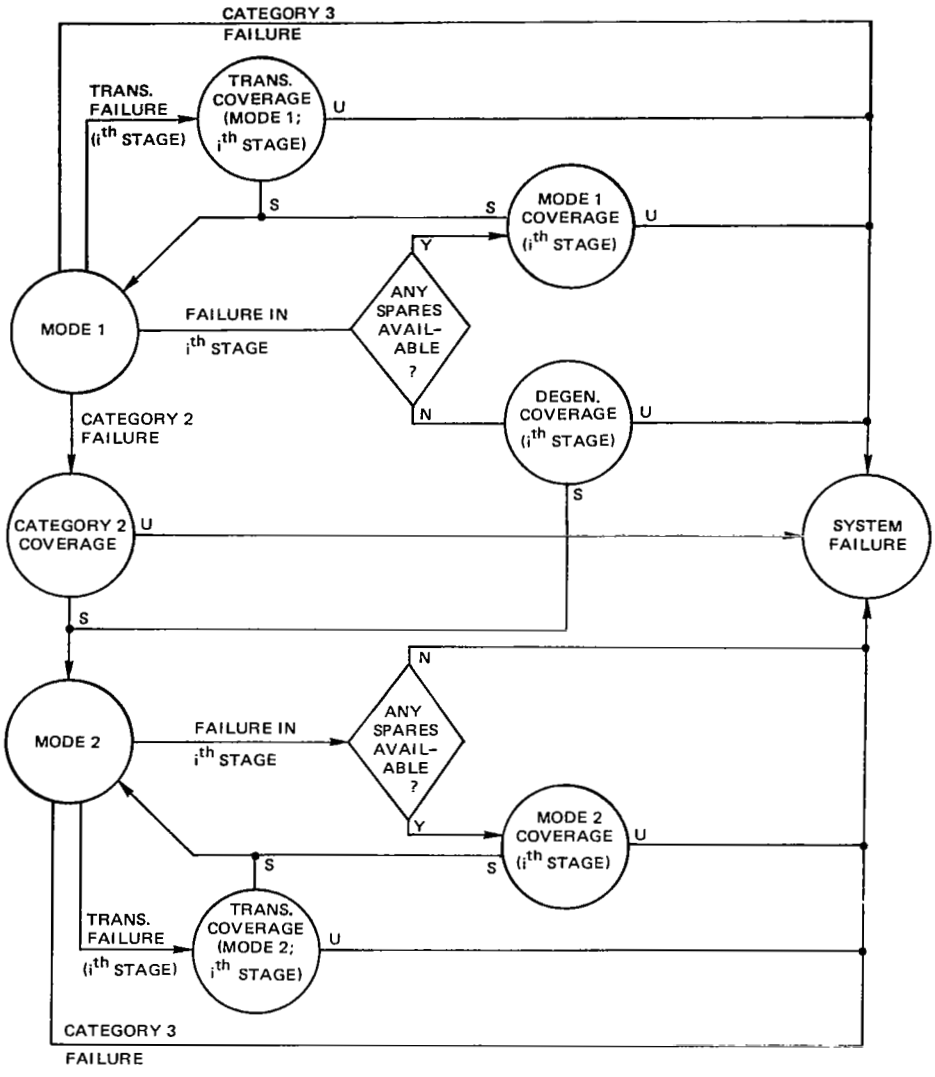


Figure 5. CARE II model.

or identify a failure and recover operation after failure. The coverage model includes the effects of failure type, number of spares that must be tested, and the dynamic effects of the recovery process.

CARE and the other programs are intended for general use. However, it was difficult to obtain sufficient information and understand the operation of the program well enough to efficiently make the modifications that are inevitable when a program is applied to a real system. CARE III had the potential for use in this study but was not operational at the time of this analysis.

Markov Analysis

Markov analysis was performed in an early stage of this reliability study using a simple preliminary model of the system. A program that had been developed at the Charles Stark Draper Laboratory (CSDL) to analyze the fault tolerant multiprocessor (FTMP) was modified, and some useful preliminary results were obtained. However, as the model for the system was perfected and expanded, the magnitude of the Markov analysis became excessive. A representative model of the total F-8 DFBW system would require thousands of states. The computational matrix would be impossibly large, and all of the required transitions would be extremely difficult to identify and compute.

The unique capabilities offered by Markov analysis were also judged to be nonessential for an analysis of the F-8 DFBW system. The Markov process has the ability to model the dynamic nature of the failure process. This is particularly important in systems that reconfigure themselves after a failure and thus become particularly vulnerable to second failures during the reconfiguration process. The F-8 DFBW system uses primarily triple redundancy that is always connected. There is very little dynamic reconfiguration except for the switch to the bypass system, which occurs after two digital system failures. In the preliminary analysis that was done, there were few cases where the actual dynamic nature of the failure process was significant. A much simpler static reliability analysis could thus be used.

Fault-Tree Analysis

Fault-tree analysis, a combinatorial analysis technique, can be a very powerful tool in analyzing system unreliability.[6] It uses a "top-down" analytical approach which can increase system visibility and significantly aid in understanding the potential failure modes in a system.

The fault tree is a graphical representation of the logical relationship between an undesired "top event" (loss of aircraft in this case) and basic failures or "primary events". The tree is constructed with a defined set of logic symbols using system data (schematics, functional flow diagrams, etc.) to determine each of the possible failures that could cause the top event. It has the advantage of displaying only those failures that lead to the top event, it can facilitate quantification of probabilities of occurrence of events, it makes subdivision of major events into lower level events easier, and it is flexible as to the degree of detail that may be used.

A fault tree was used during the preliminary reliability analysis of the F-8 DFBW system, and the basic principles of the fault tree were used during this study to aid in the understanding of the failure modes. Attempts to develop a complete fault tree for the total system, however, became very involved. There were two major difficulties. One was assuring that all combinations of subsystem failures that can lead to system failure were identified. For example, it is easy to identify the failure of all three inverters or the failure of the required number of actuators in a particular axis as a system failure mode. It is much more difficult to assure identification of all failure modes that are caused by inverter failure in one channel and actuator failures in other channels. This situation is illustrated by the segment of a fault tree shown in Figure 6.

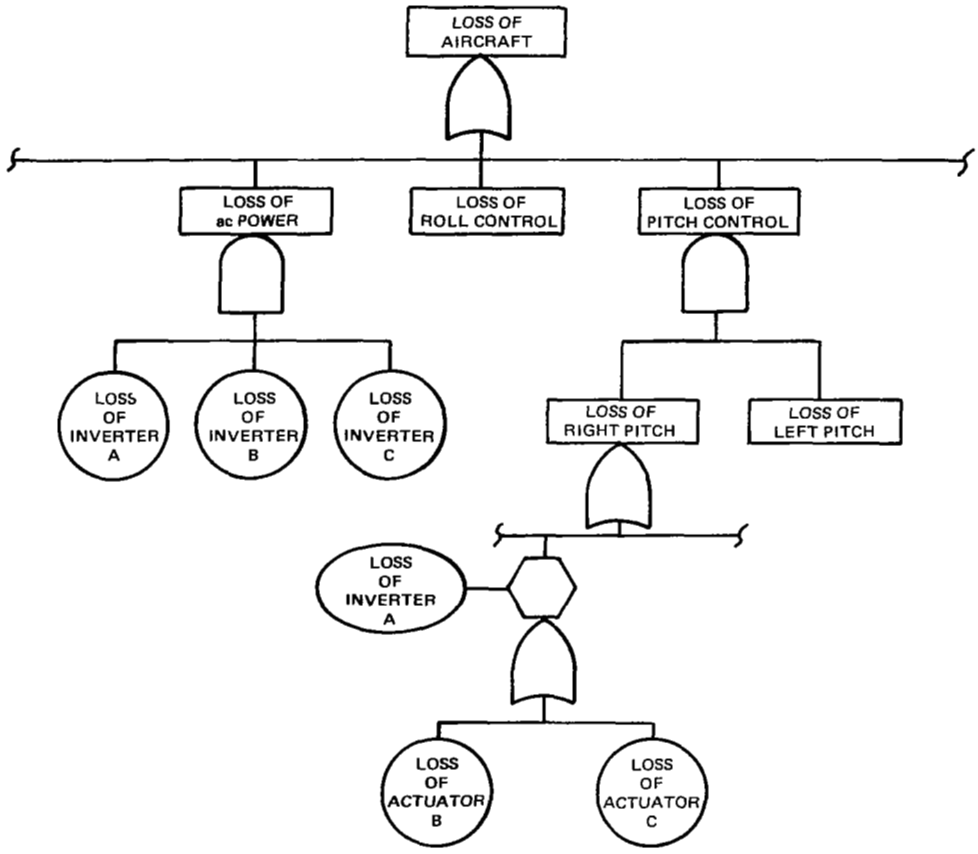


Figure 6. Part of a system fault tree.

The other major difficulty was assuring that all dependent events could be handled properly. Many primary events contribute to system failure by combining in different ways with other primary events. This difficulty is also illustrated in Figure 6, where the event "loss of inverter A" appears twice (and, in fact, would appear many times in the total diagram). These multiple events can be accounted for by creating an equivalent fault tree by Boolean manipulation to reduce the fault tree to a diagram where all primary events appear only once.

It was assumed that with sufficient effort it would indeed be possible to construct an accurate fault tree for the F-8 DFBW system. However, it was foreseen as a formidable task to construct the initial fault tree and even more difficult to reduce the tree to a form from which equations could be written easily. This situation led to the investigation of other methods which appeared to be more effective.

Conventional Combinatorial Analysis

The classical combinatorial reliability analysis as described in Appendix A of MIL-HDBK-217C [7] was considered as an alternative for the F-8 DFBW analysis. The normal procedure for constructing a reliability model using this method is:

(1) Define the requirements for mission success in a mission-success diagram.

(2) Write the probability-of-survival equation for the system based on the mission-success diagram.

(3) Calculate the probability of success for each of the individual elements of the system identified by the diagram and equation.

(4) Insert these probability numbers into the equation and calculate the system reliability.

The mission-success diagram is a serial, parallel, and hybrid arrangement of basic system elements that define all paths that lead to system success. Success diagrams were drawn for various parts of the F-8 DFBW system. However, the same kinds of difficulties were encountered in constructing a complete and accurate diagram as were

encountered in constructing the fault tree. The diagram became very involved, particularly for elements that are common to many different success paths.

A portion of a mission success diagram is shown in Figure 7. This shows how the generator, batteries, and inverters are involved in both the pitch and roll bypass systems. These same elements are also involved in the primary digital system and all of the actuators. The complete diagram would thus become highly unmanageable and very difficult to confirm as accurate.

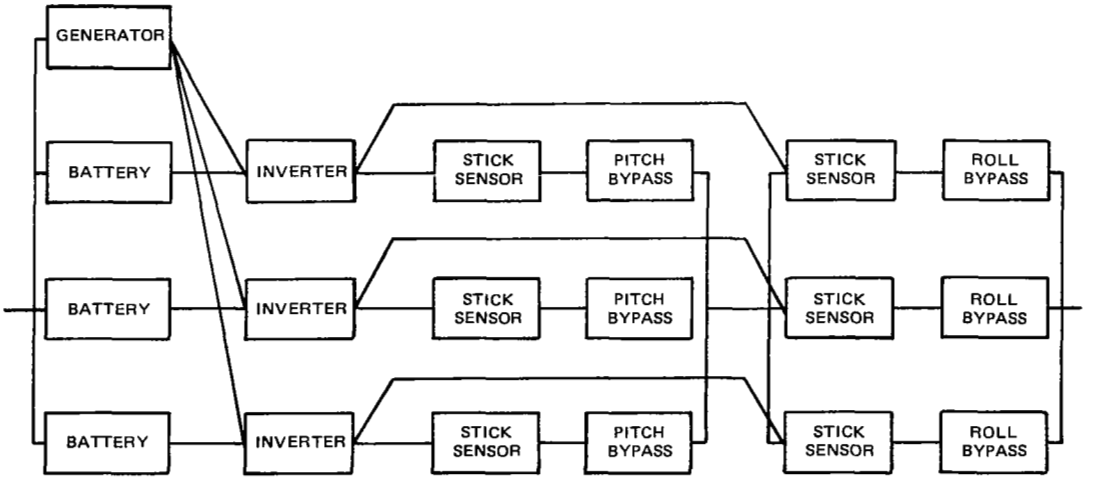


Figure 7. Part of a mission success diagram.

The development of the basic reliability equation as described in MIL-HDBK-217C is reasonably well understood, and is a particular case of Bayes' theorem based on the product laws of probability. It is:

$$P_S = P_S \text{ (if X is good) } R_X + P_S \text{ (if X is bad) } Q_X \qquad (1)$$

where

P_S = reliability of mission

P_S (if X is good) = reliability of mission if X is good

P_S (if X is bad) = reliability of mission if X is bad

R_X = reliability of X

Q_X = unreliability of X = 1 - R_X

In other words, the reliability of the mission is equal to the reliability of the mission given that a specific portion of the system works times the probability that a portion of the system will work plus the reliability of the mission given that a specific portion of the system fails times the probability that that portion fails.

This basic equation was used in MIL-HDBK-217C to develop the standard reliability equations for series, parallel, and series-parallel combinations of equipment, but it stated that for non-series-parallel or complex configurations, repeated use of the equation is required. The F-8 DFBW certainly falls in the category of a complex system for which no standard equation can be easily applied.

In many cases it was found that the equations being used to check the mission-success diagram were better understood than the diagram. It was thus attempted to write the equations for the total system directly. The total set of equations, however, covered many pages and became very cumbersome. The notation for the equations became awkward and the interrelationship among equations was difficult to show. This situation led to the ideas that became the basis for the technique finally used to perform the analysis.

This technique was a graphical presentation of the basic reliability equations. This type of diagram is related to a fault-tree diagram or a mission-success diagram, but is not exactly the same as either. It does, however retain the advantage of these other diagrams in that visibility and understanding of system operation is enhanced. The following section gives a description of the technique developed for analyzing the reliability of the F-8 DFBW system.

Random-Failure Analysis Technique

Basic Reliability Equation

The basic reliability equation used in this analysis is related to Bayes' theorem, and is more general than the one used in MIL-HDBK-217C (Eq. (1)). The general form of the equation can handle redundant systems more efficiently. It gives the unreliability of the system as a sum of terms related to a set of mutually exclusive events. Each term is the product of the probability of one of the events and the conditional unreliability of the system given the occurrence of that event. The equation is thus:

$$Q(S) = Q(S|A)P(A) + Q(S|B)P(B) + Q(S|C)P(C) + \ldots \qquad (2)$$

where

$Q(S)$ = unreliability of the system

$Q(S|A)$ = unreliability of the system given event A

A,B,C, ... = events describing the state of the system relative to the operation of the hardware at a particular level. For example:

A = all three hydraulic systems working

B = one system failed, others working

C, ... = other events that complete the set

$P(A)$ = probability of event A

Conditions which must be met are

$$P(A) + P(B) + P(C) + \ldots = 1$$ (exhaustive list of events that spans the space)

$$P(AB) = P(AC) = P(BC) = \ldots = 0$$ (all events are mutually exclusive)

Figure 8 is a diagram of Eq. (2). The equation could have been written as easily for reliability, but unreliability is used for numerical computation reasons, as will be explained later.

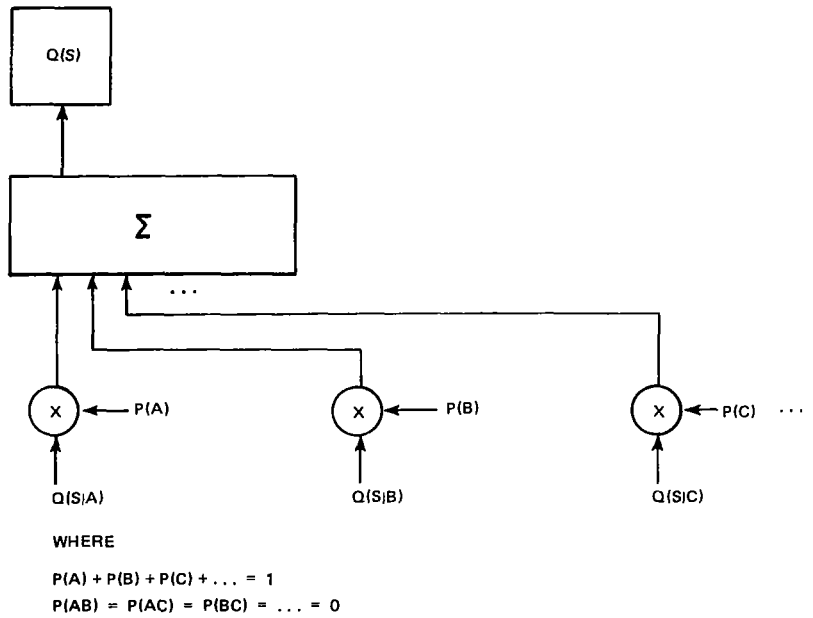


Figure 8. Graphical equivalent of basic equation.

Equation (1) (used in MIL-HDBK-217C) is a special case of Eq. (2) as it is based on only one piece of equipment. For example, in the equation related to the flight-control generator, event A would be when the generator is good and event B would be when generator is bad. No other events would be involved and thus the conditions are met. The generator must be either good or bad with a probability of 1, and it cannot be both good and bad.

Steps in Applying the Equation to a System

The steps which were used in applying the equation to the system are as follows:

Step 1: Partition the system into basic elements.

The system must be divided into a number of basic elements. In order for the analysis to be as simple as possible, the number of elements should be as small as possible as long as the total system is accurately represented. The elements are essentially defined by the random-failure containment boundaries. In other words, the boundaries are made as large as possible as long as any failure within the element prevents any other part of the element from being used. In general, boundaries must be drawn at any point where there is cross-coupling between channels.

Step 2: Select order in which the equations will be applied to the basic elements.

Once the system has been divided into its basic elements, an order must be chosen for the application of Eq. (2). The order in some cases can be somewhat arbitrary, but the resulting equations can differ greatly in complexity. The order essentially has to reflect the chain of dependencies. An element that depends on another element should be placed after it in the sequence. The power sources will thus tend to be first, with other elements arranged essentially in the order of signal flow. The final order is based on practical experience and trial and error.

Step 3: Construct diagram of equations.

Equation (2) is applied, element by element, by constructing a diagram showing the interrelationship between equations. At each level, the set of events that define the state of the system for that element must be defined. It must be assured that the completeness and exclusiveness conditions are met for these events.

It is also necessary that the events that create a unique system configuration for the remaining elements be differentiated. In many cases it may not be important which particular element in a triplex set fails. For example, the state of the system may be the same independent of which ac power supply fails. In this case, an event can be defined as the failure of any one of three power supplies, with the appropriate probability of the event. In other cases, there may be some distinction between channels. For example, in determining the probability of loss of aircraft, it makes a difference which hydraulic systems have failed. There is also often a need to make a distinction between two different types of elements on the basis of whether they have failed in the same channel or in different channels.

The inputs to the equation at each level are the unreliabilities of the system due to failures in all following elements; this is conditioned upon the state of the system as it is defined by preceding levels. The diagram thus grows geometrically at each level. The total diagram and the equations it represents would become completely unmanageable if it were not for the fact that many of the necessary conditional unreliabilities are equivalent and do not need to be computed more than once. The construction of the diagram and the economies that can be achieved are more clearly understood within the context of actual application to the F-8 system (see the next subsection).

Step 4: Compute the probabilities for each event.

At each level, the probabilities for each event must be computed. These probabilities will be a function of the reliability of the basic element. For example, for a triplex element, the probability of the event "all three good" would be the reliability of the basic element cubed. The probability of other events would be similar functions of the reliability or unreliability of the basic elements.

The failure rate of each basic element is obtained from the most accurate sources available. The best source would be actual experience on the element as long as there was enough experience for it to be statistically significant. Other sources of this reliability data are actual experience on similar parts and reliability predictions based on procedures such as those outlined in MIL-HDBK-217C. The development of the basic failure rates for the elements making up the F-8 DFBW system are given in Section 5.

Step 5: Compute system unreliability.

The final step in the system analysis is to insert the basic element failure rates into the resulting total unreliability equation, and compute the system unreliability. For a reasonably sized system, this computation could be done manually. For larger systems, and also to allow unreliability to be computed many times for different element failure rates and different system configurations, machine computation can be effective. A computer program was written for the F-8 DFBW system analysis. This program is described in Section 4 and the results are given in Section 6.

Application of Analysis Technique to the F-8 DFBW

Partition the System

The F-8 DFBW system was partitioned into 19 different categories of elements; all except the generator are triplex. Table 1 lists the elements; Figure 9 shows the total system diagram. The operation of the system is described in Appendix B. The F-8 aircraft does not require active stability augmentation; thus inertial and air data sensors are not included in the analysis.

Table 1. Basic system elements for the F-8 DFBW.

Hydraulic systems	Two primary and one utility
Generator	One dedicated to the flight-control system
Batteries	Three—one dedicated to each channel
Inverters	Three 26-V 400-Hz supplies for the linear variable differential transformers (LVDTs)
Primary digital system (PDS)	Three—includes computer, interface unit (IFU), stick and pedal sensors, and interface circuits in the backup and servo electronics (BASE)
Backup and servo electronics	Three each of 14 different elements

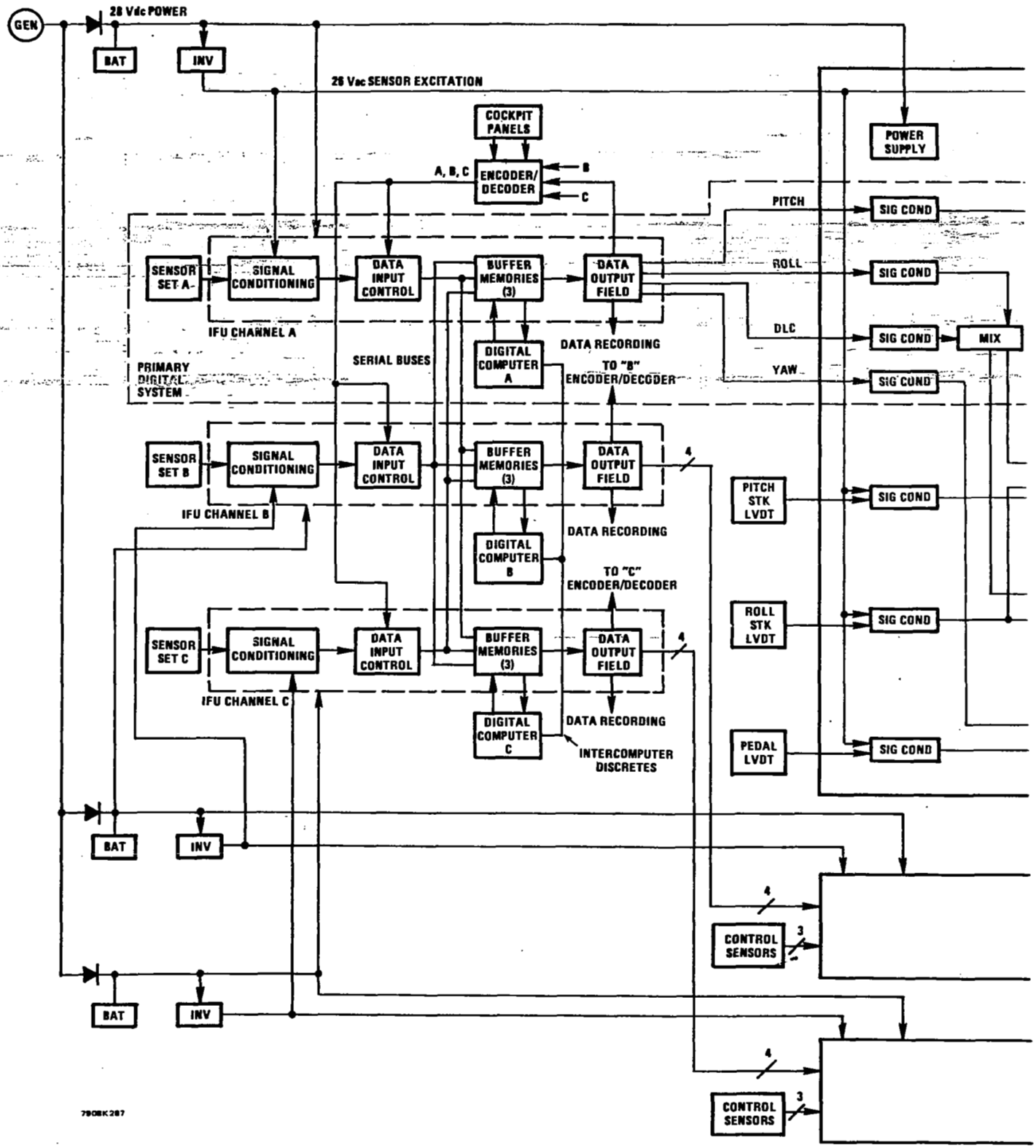
The hydraulic power system is divided into three elements. Two primary hydraulic systems supply power to the primary hydraulic actuators and wing spoiler. There is one utility system that supplies hydraulic power to the landing gear, steering, speed brakes, etc. One of these three hydraulic systems supplies power to each channel of the triplex secondary actuator, which was added to the aircraft as part of the flight-control experiment. The hydraulic power system includes all of

the components such as pumps, reservoirs, tubes, and connectors up to the "ON" solenoid for each channel of the secondary actuators. It is assumed that a failure in any one of these components will cause loss of hydraulic power to all actuators connected to that system.

Electrical power has been divided into three categories of elements. There is one generator that was added to the aircraft to supply power to the electronic flight-control system. The generator is backed up by three batteries that are dedicated to each channel. Another critical power-supply element is the inverter. There are three inverters, one dedicated to each channel, that provide 26-volt 400-Hz excitation for all LVDTs, both for the stick and pedal inputs and for the position feedbacks on the secondary actuators.

The primary digital system is taken as one failure element. It combines all the parts within the dotted line labeled "Primary Digital System" in Figure 9, and includes the digital computer, the IFU, the stick and pedal sensors, and the signal conditioning circuits within the BASE that receive the surface command signals from the IFU. All of these parts can be combined into one element because, in almost all cases, the failure of one part prevents the use of any other part. One exception is the first failure of a pilot control input. Sensor inputs are exchanged between channels through the IFU. Thus, the first failure of a pilot input sensor does not prevent the rest of that digital channel from being used. However, the sensor inputs from each channel are dependent on the operation of that digital channel. If that digital channel fails, the sensors associated with that channel are lost to all channels. Thus, a second failure either in a pilot input sensor or any other part of another digital channel will cause two of three sensor inputs to be lost to all channels, leading to loss of the digital mode. The effect is thus essentially the same as if the first sensor failure had caused the loss of the whole associated digital channel. The inclusion of pilot inputs within the digital channel failure element thus simplifies the analysis, while leading to a slightly conservative system reliability estimate. As will be seen in Section 5, the contribution of pilot inputs to the digital system is numerically negligible.

Each BASE unit was divided into 15 different parts. One part is included within the primary digital system element, and the remainder adds 14 different elements to the analysis. These elements are listed in Table 2. There are some components that are common to the entire BASE unit which are assumed here to be contained in the power supplies.


GEN
28 Vdc POWER
BAT
INV
26 Vac SENSOR EXCITATION
COCKPIT PANELS
A, B, C
ENCODER/ DECODER
B
C
POWER SUPPLY
PITCH
SIG COND
ROLL
SIG COND
DLC
SIG COND
MIX
YAW
SIG COND
SENSOR SET A
SIGNAL CONDITIONING
DATA INPUT CONTROL
BUFFER MEMORIES (3)
DATA OUTPUT FIELD
IFU CHANNEL A
DIGITAL COMPUTER A
DATA RECORDING
TO "B" ENCODER/DECODER
PRIMARY DIGITAL SYSTEM
SERIAL BUSES
SENSOR SET B
SIGNAL CONDITIONING
DATA INPUT CONTROL
BUFFER MEMORIES (3)
DATA OUTPUT FIELD
4
IFU CHANNEL B
DIGITAL COMPUTER B
DATA RECORDING
TO "C" ENCODER/DECODER
PITCH STK LVDT
SIG COND
ROLL STK LVDT
SIG COND
SENSOR SET C
SIGNAL CONDITIONING
DATA INPUT CONTROL
BUFFER MEMORIES (3)
DATA OUTPUT FIELD
4
IFU CHANNEL C
DIGITAL COMPUTER C
DATA RECORDING
INTERCOMPUTER DISCRETES
PEDAL LVDT
SIG COND
BAT
INV
4
CONTROL SENSORS
3
BAT
INV
4
CONTROL SENSORS
3
79DBK287

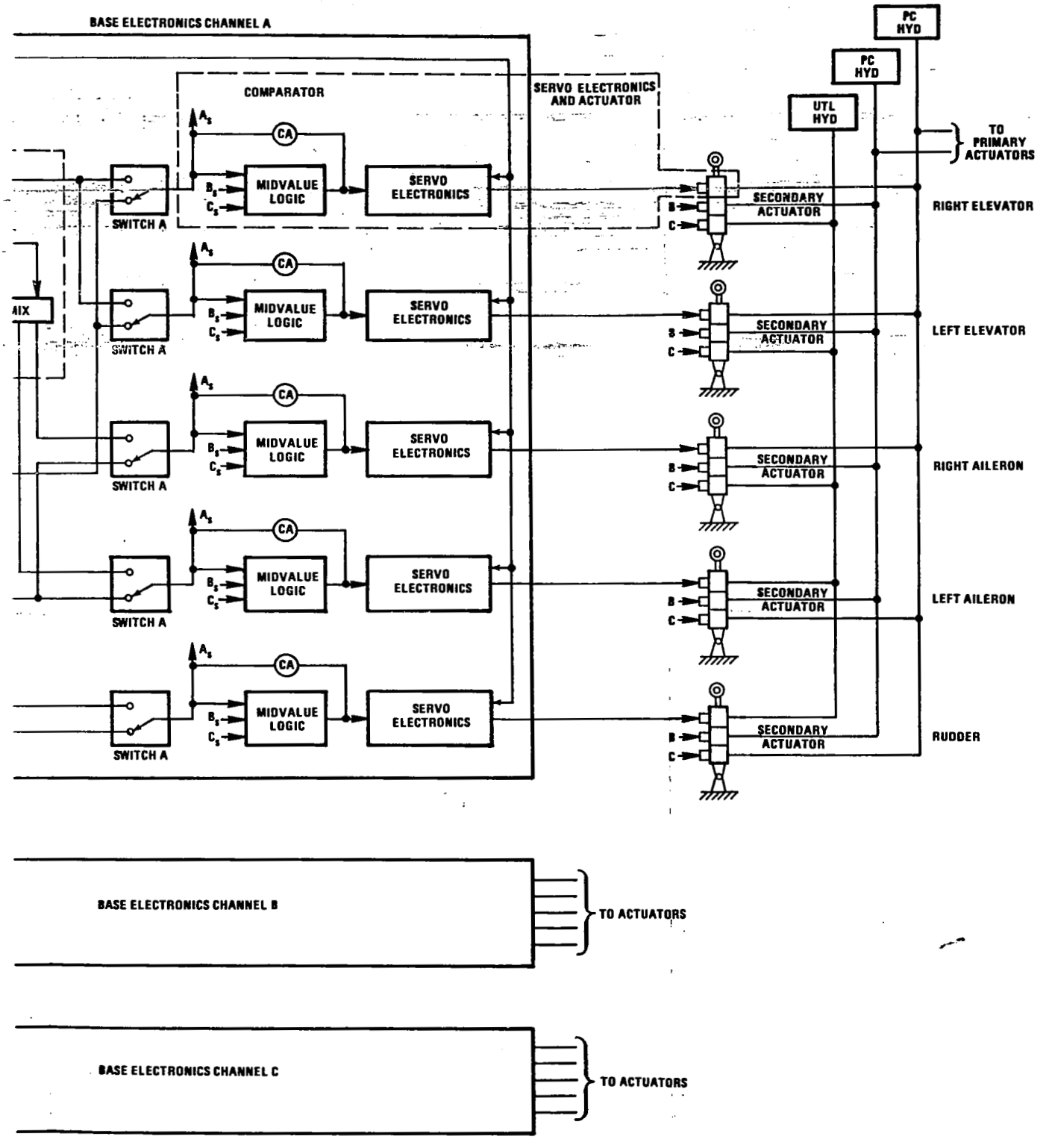


Figure 9. F-8 DFBW system diagram

Table 2. Backup and servo electronics partitioning.

Common BASE electronics (primarily the power supply)
Computer bypass electronics Pitch, including stick sensor Roll, including stick sensor Yaw, including pedal sensor
Primary digital system/computer bypass system (PDS/CBS) switch Right and left pitch Right and left roll Yaw
Servo electronics and actuator Includes: Midvalue-select circuit Comparator Logic Servo electronics One selection of the triplex secondary actuator For each: Right and left pitch Right and left roll Yaw

If there is a failure within the common BASE electronics element (assumed to be primarily the power supplies common to all BASE parts), the entire BASE unit will be lost.

The BASE computer bypass electronics is comprised of three elements, which provide a direct connection between the pilot control sensors and the actuator commands. The pitch, roll, and yaw circuits are independent, and include input signal conditioning, signal shaping, and synchronization circuits to ensure a smooth transition when the system is switched from the primary digital system to the bypass system.

Five elements are required for the primary-digital-system-to-bypass-system switch. This switch is a small element, but it plays an important role and cannot be accurately combined with any other element because of the way in which the system is partitioned and cross-coupled. The remaining five elements in the BASE units include the midvalue-select circuit; the comparator; the servo amplifier; and the delta pressure (Δp)

midvalue select, equilization, and comparator. All logic within the BASE units has also been included in this element, because a failure in logic would primarily affect the actuator commands. One channel of the triplex secondary actuator is also included in this element. The actuator can be included because a servo-electronics failure will cause loss of the use of that actuator, making the electronics useless.

Select the Order of the Elements

The order selected for elements is given in Table 3. In most cases the order is determined by the sequence of dependencies. In other cases, the choice is somewhat arbitrary. Hydraulic power was

Table 3. Order selected for applying equations to elements.

1	Hydraulics
2	Generator
3	Batteries
4	Inverters
5	Common BASE Electronics
6	Primary Digital System
7	Pitch Bypass
8	Right Pitch Switch
9	Right Pitch Actuation
10	Left Pitch Switch
11	Left Pitch Actuation
12	Roll Bypass
13	Right Roll Switch
14	Right Roll Actuation
15	Left Roll Switch
16	Left Roll Actuation
17	Yaw Bypass
18	Yaw Switch
19	Yaw Actuation

placed first simply because it was somewhat complex, and by putting it first, it would have to be written only once. If it were placed later in the sequence, it would have to be reproduced for each conditional state that was generated by the previous elements. The generator was placed before the batteries because if the generator is good, the batteries are not needed. The ac inverter is next as it depends on the generator or battery. All of these power supplies are first because the rest of the equipment depends on them.

The common BASE electronics is placed before the primary digital system because the loss of this element will cause the output from the digital system to be lost from all other channels, and will thus be equivalent to the loss of a digital channel. The primary digital system is placed before the bypass element of the BASE because, if the digital system is good, the bypass is not needed.

The switch and then actuation elements for each system axis are placed together to simplify the resulting equations. All switches could have been placed first and followed by all actuation, but the resulting diagram and equations would have been much more complex.

Construct Diagram of the Equations

The total equation for the unreliability of the system due to random component failures can now be formed by constructing a diagram for the equations. This diagram is presented in five sections in Figure 10. The first section covers the first 6 elements, and the other 4 sections cover the remaining 13 elements for different system states as determined by failures in the first 6 elements. This diagram is not described in detail. However, typical parts are described so that the methods used for developing the diagram can be understood.

The equation for the first element (hydraulic power) is

$$\begin{aligned} Q(S) = {} & Q(S \mid 3HYD)P(3HYD) + Q(S \mid 2HYD, \overline{HYD})P(2HYD, \overline{HYD}) \\ & + Q(S \mid PC, \overline{PC}, \overline{UTL})P(PC, \overline{PC}, \overline{UTL}) \\ & + Q(S \mid UTL, 2\overline{PC})P(UTL, 2\overline{PC}) + Q(S \mid 3\overline{HYD})P(3\overline{HYD}) \end{aligned}$$

where a bar over a symbol means the element has failed and the number indicates how many channels are good or bad (e.g., P(3HYD) denotes the probability that all three hydraulic systems are good). This is the application of the general equation (Eq. (2)), giving the unreliability of the system as a function of the state of the hydraulic power.

Five states for the hydraulic power are defined. The first is that all three hydraulic power supplies are good. The second is that any two of the three supplies are good and one is failed. This event can happen in three different ways by the failure of any one of the three supplies. These different ways can be combined into one event because the unreliability of the remainder of the system is equivalent no matter which supply has failed. When two supplies fail, a distinction must be made as to which two have failed. As long as one primary hydraulic system is still good, the aircraft can be flown; however, if both primary hydraulic systems fail, the aircraft cannot be flown since the primary systems power the primary actuators. Two events are thus defined for two hydraulic failures:

(1) One primary system is good and the other two systems have failed, which can happen two ways.

(2) Only the utility system is good.

The final event is that all three hydraulic systems have failed.

If it is assumed that all three hydraulic systems have the same reliability [R(HYD)], the probability of the five events will be as follows, where Q(HYD) = 1 - R(HYD)

$$P(3HYD) = R(HYD)^3$$

$$P(2HYD, \overline{HYD}) = 3R(HYD)^2 Q(HYD)$$

$$P(PC, \overline{PC}, \overline{UTL}) = 2R(HYD)Q(HYD)^2$$

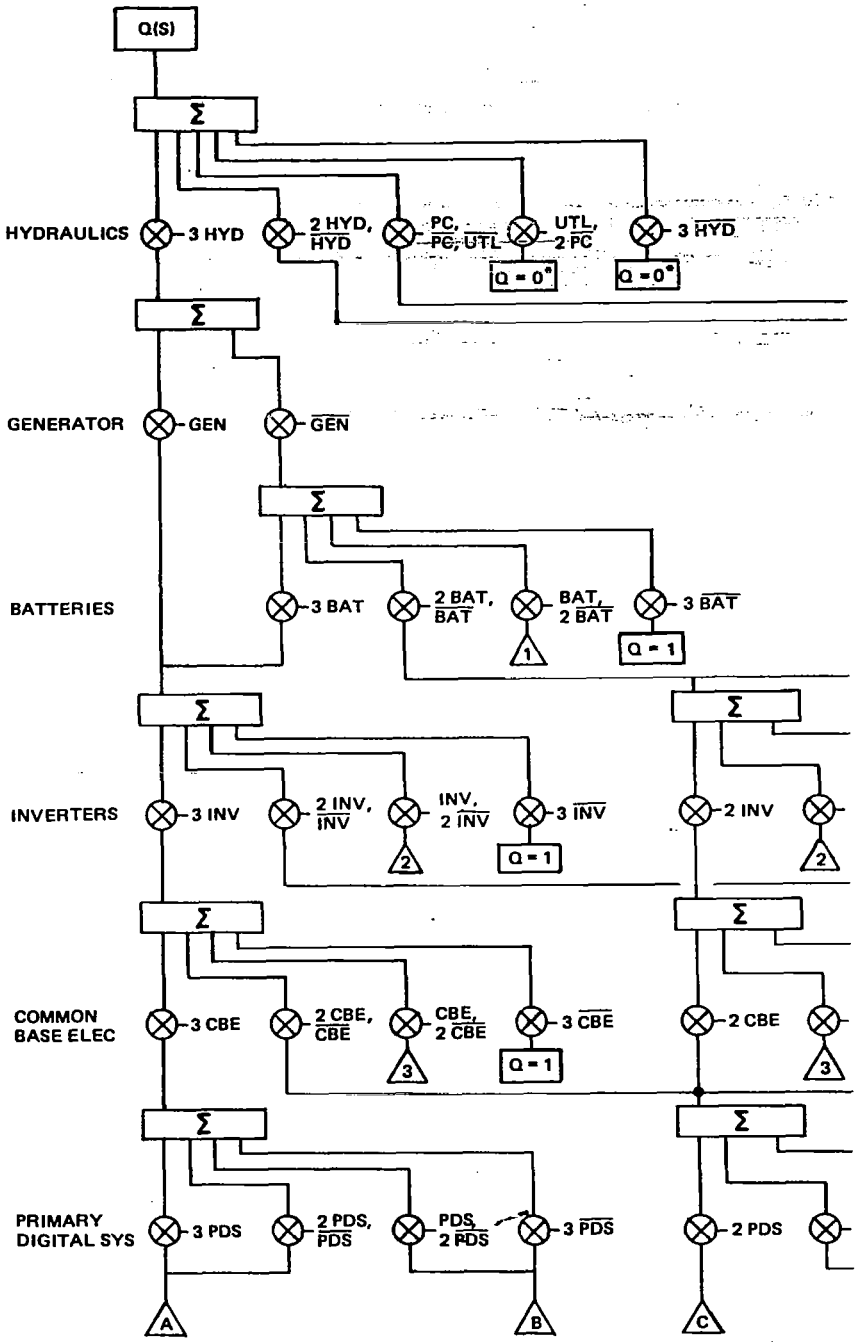
$$P(UTL, 2\overline{PC}) = R(HYD)Q(HYD)^2$$

$$P(3\overline{HYD}) = Q(HYD)^3$$

The completeness condition for these events can be shown by the addition

$$\begin{aligned} R^3 + 3R^2Q + 2RQ^2 + RQ^2 + Q^3 &= R^3 + 3R^2Q + 3RQ^2 + Q^3 \\ &= (R + Q)^3 \\ &= 1 \end{aligned} \qquad (3)$$

where R and Q are the system reliability and unreliability, and R + Q = 1 by definition. The mutual exclusiveness condition is shown by inspection of each pair. It is impossible for all three to be good and one to be bad and so forth.



*LOSS OF AIRCRAFT DUE TO COMPLETE HYDRAULIC FAILURE NOT ALLOCATED TO ELECTRONIC FLIGHT-CONTROL SYSTEM.

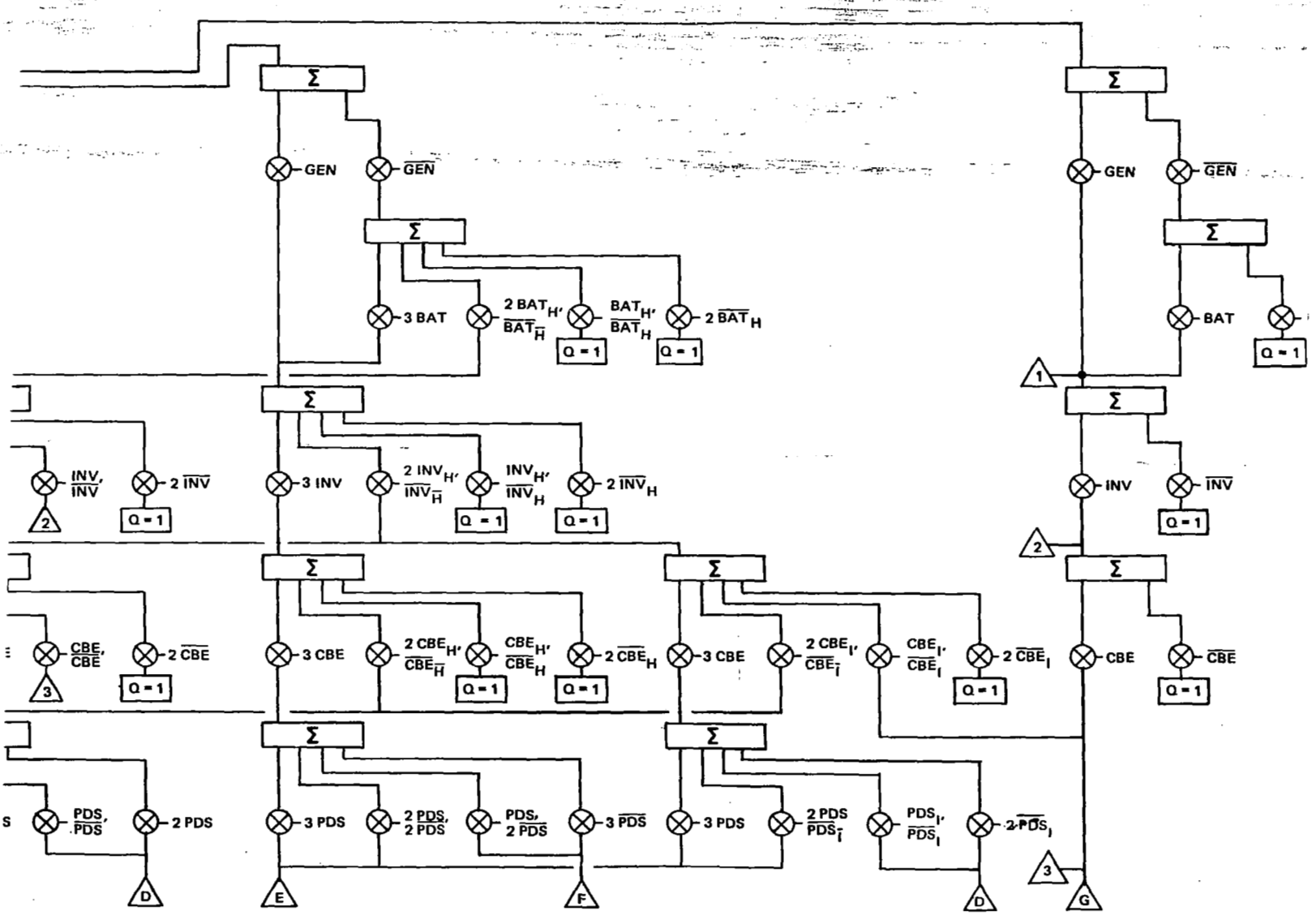
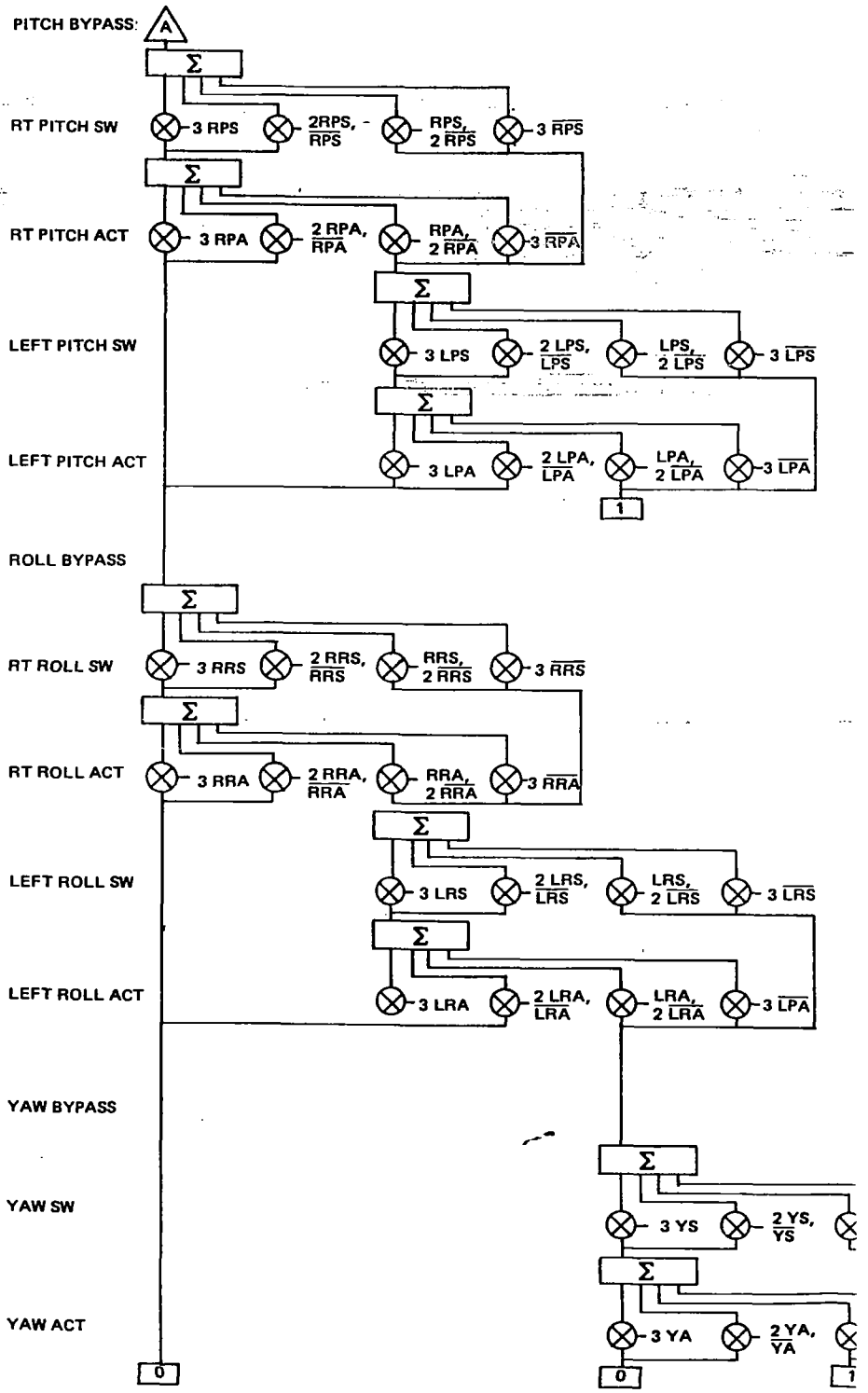


Figure 10a. Diagram of F-8 DFBW
reliability equation


PITCH BYPASS
A
Σ
RT PITCH SW
3 RPS
2RPS, RPS
RPS, 2 RPS
3 RPS
Σ
RT PITCH ACT
3 RPA
2 RPA, RPA
RPA, 2 RPA
3 RPA
Σ
LEFT PITCH SW
3 LPS
2 LPS, LPS
LPS, 2 LPS
3 LPS
Σ
LEFT PITCH ACT
3 LPA
2 LPA, LPA
LPA, 2 LPA
3 LPA
1
ROLL BYPASS
Σ
RT ROLL SW
3 RRS
2 RRS, RRS
RRS, 2 RRS
3 RRS
Σ
RT ROLL ACT
3 RRA
2 RRA, RRA
RRA, 2 RRA
3 RRA
Σ
LEFT ROLL SW
3 LRS
2 LRS, LRS
LRS, 2 LRS
3 LRS
Σ
LEFT ROLL ACT
3 LRA
2 LRA, LRA
LRA, 2 LRA
3 LPA
YAW BYPASS
Σ
YAW SW
3 YS
2 YS, YS
Σ
YAW ACT
3 YA
2 YA, YA
0
0

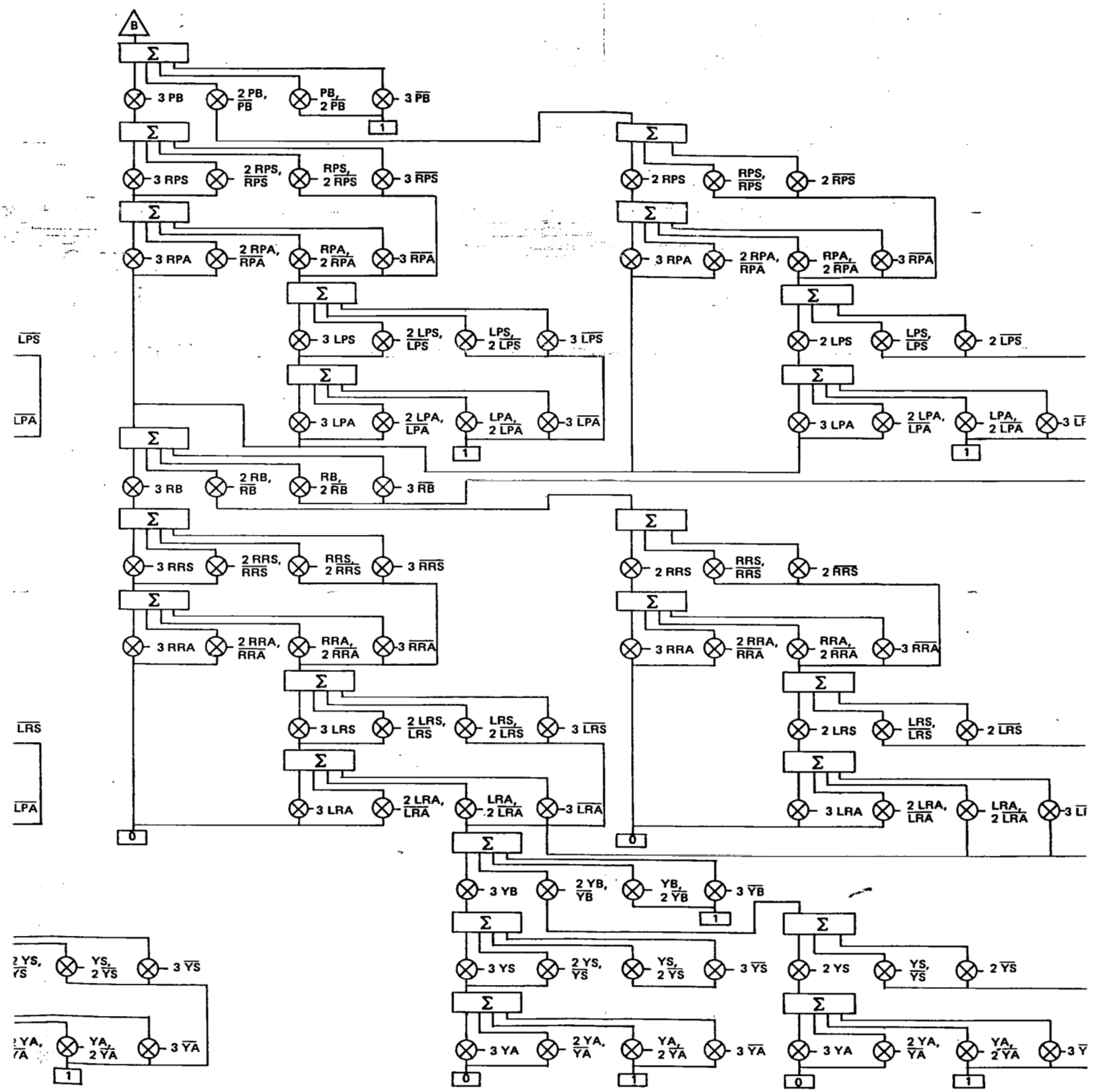
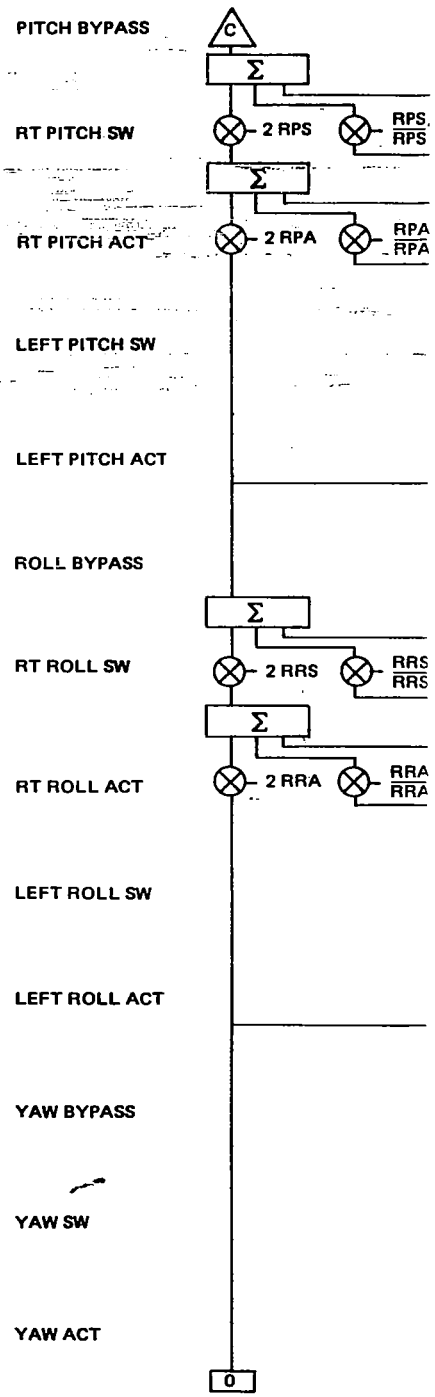


Figure 10b. Diagram of F-8 DFBW un
reliability equations.


PITCH BYPASS
C
Σ
RT PITCH SW
2 RPS
RPS
RPS
Σ
RT PITCH ACT
2 RPA
RPA
RPA
LEFT PITCH SW
LEFT PITCH ACT
ROLL BYPASS
Σ
RT ROLL SW
2 RRS
RRS
RRS
Σ
RT ROLL ACT
2 RRA
RRA
RRA
LEFT ROLL SW
LEFT ROLL ACT
YAW BYPASS
YAW SW
YAW ACT
0

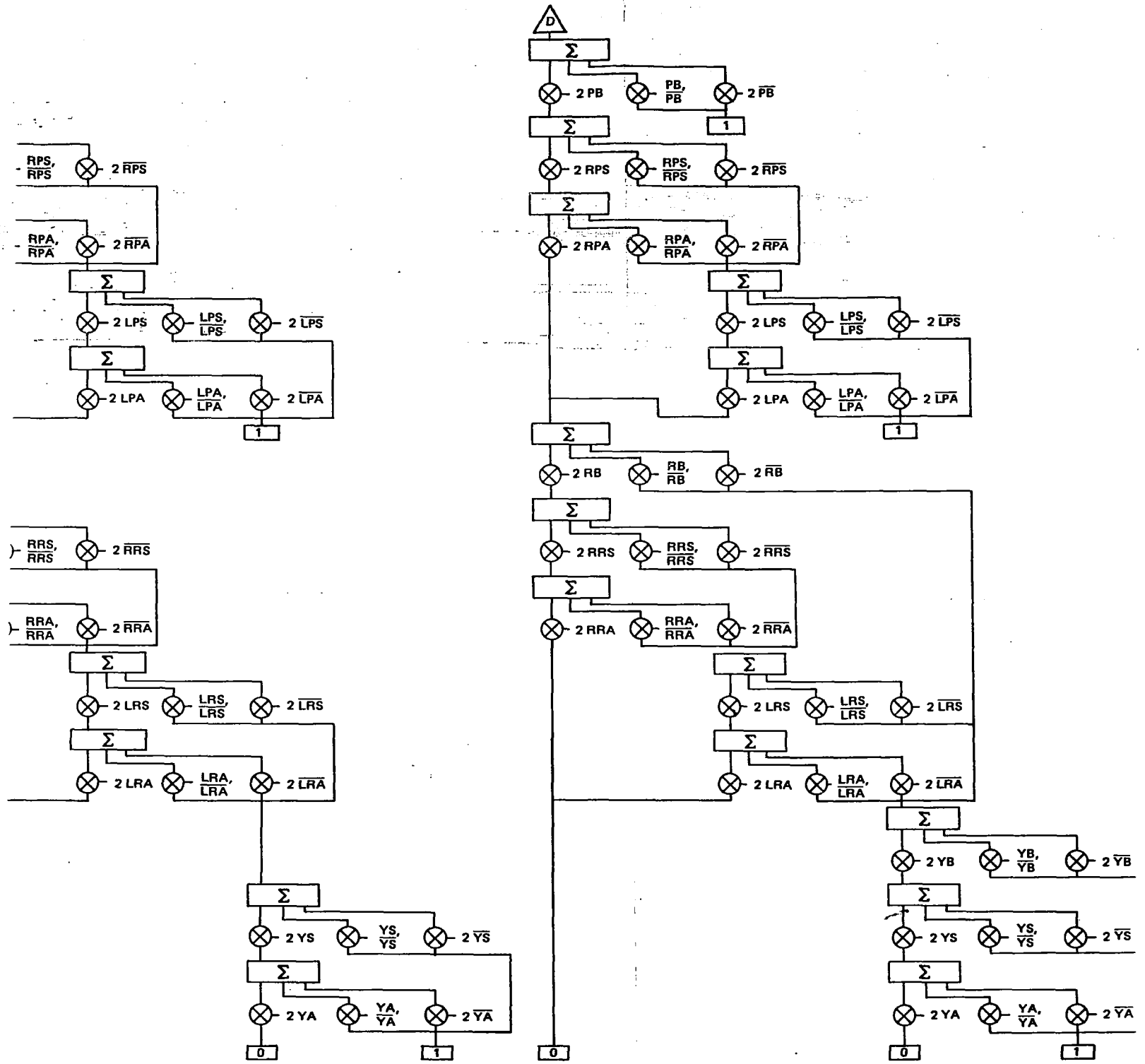
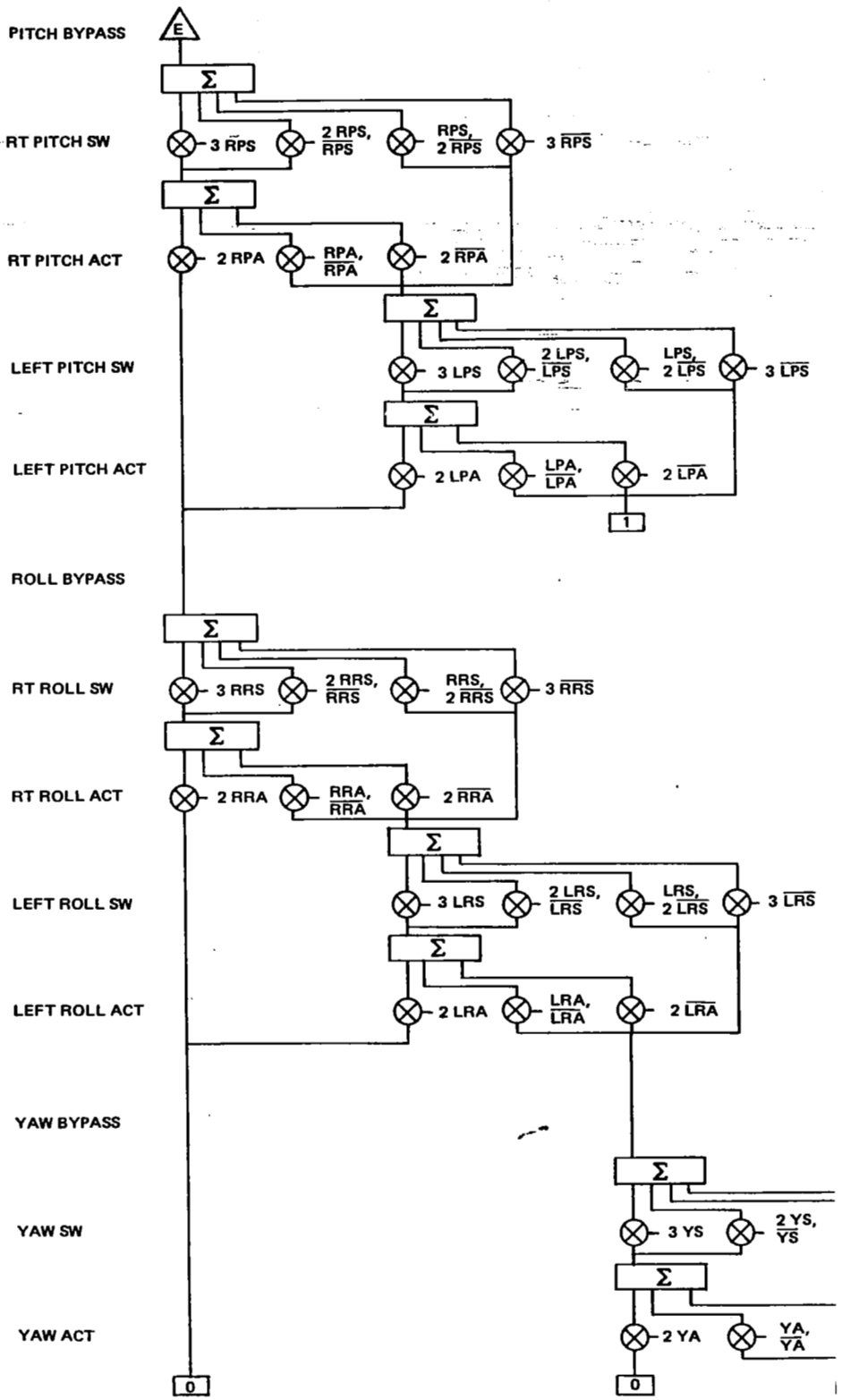


Figure 10c. Diagram of F-8 DFBW u
reliability equations


PITCH BYPASS
E
Σ
RT PITCH SW
3 RPS
2 RPS, RPS
RPS, 2 RPS
3 RPS
Σ
RT PITCH ACT
2 RPA
RPA, RPA
2 RPA
Σ
LEFT PITCH SW
3 LPS
2 LPS, LPS
LPS, 2 LPS
3 LPS
Σ
LEFT PITCH ACT
2 LPA
LPA, LPA
2 LPA
1
ROLL BYPASS
Σ
RT ROLL SW
3 RRS
2 RRS, RRS
RRS, 2 RRS
3 RRS
Σ
RT ROLL ACT
2 RRA
RRA, RRA
2 RRA
Σ
LEFT ROLL SW
3 LRS
2 LRS, LRS
LRS, 2 LRS
3 LRS
Σ
LEFT ROLL ACT
2 LRA
LRA, LRA
2 LRA
YAW BYPASS
Σ
YAW SW
3 YS
2 YS, YS
Σ
YAW ACT
2 YA
YA, YA
0
0

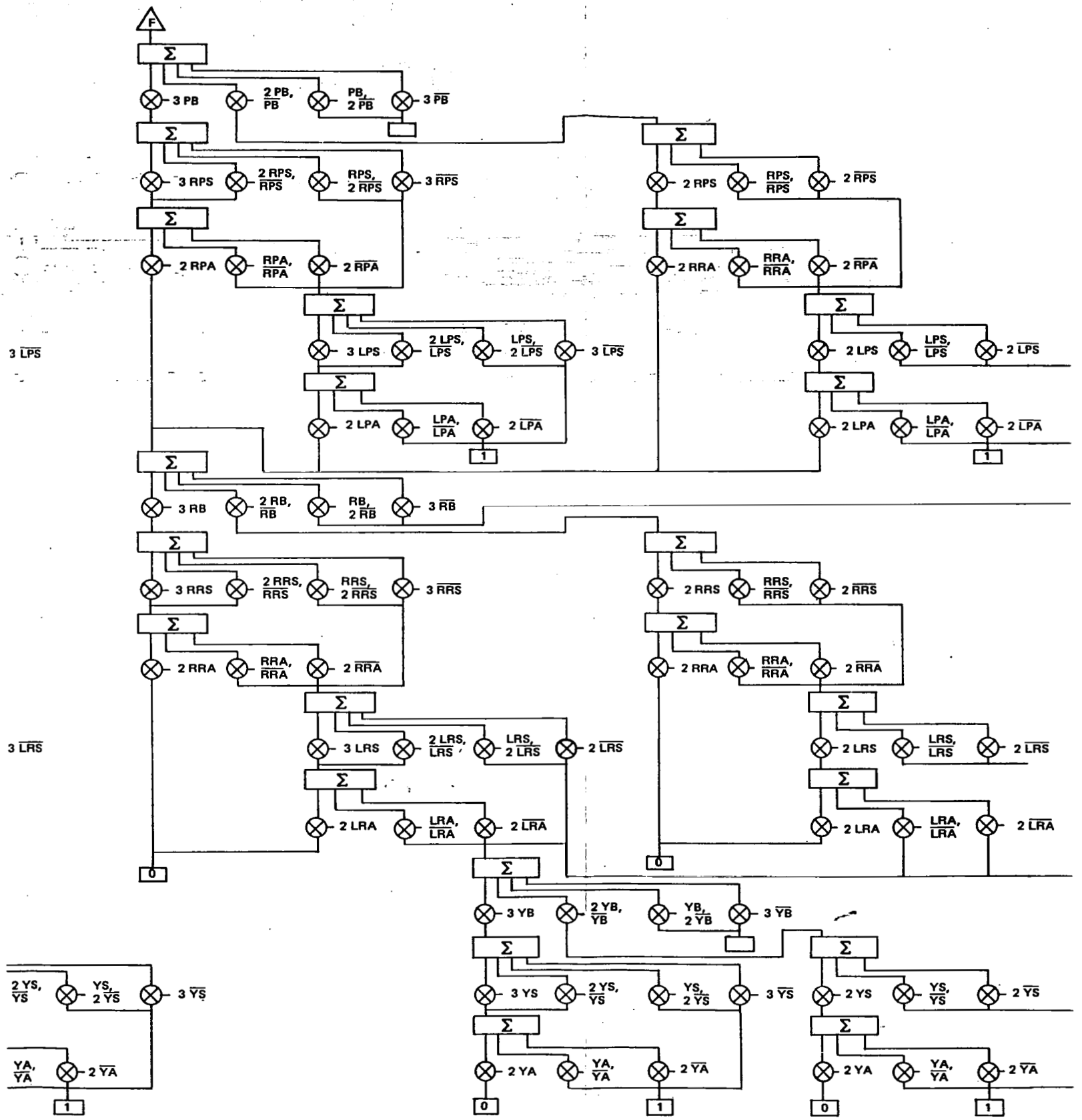


Figure 10d. Diagram of F-8 DFBW unreliability equations.

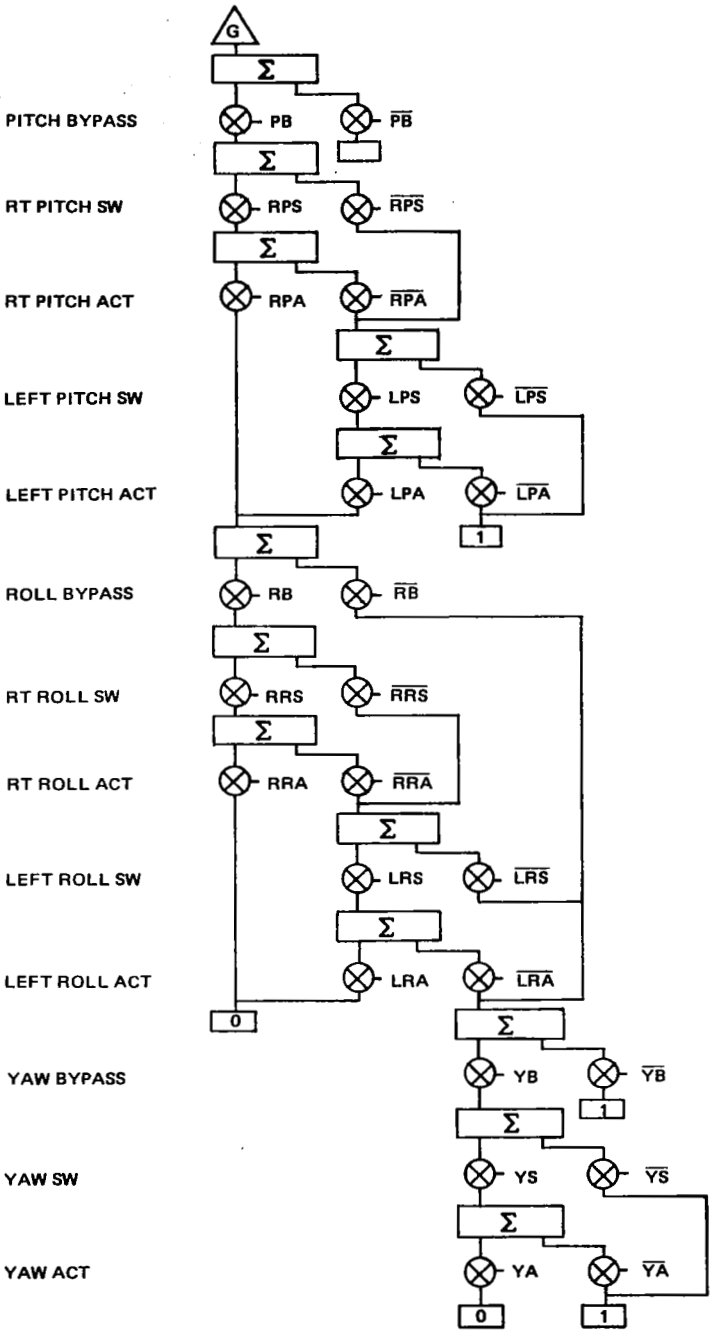


Figure 10e. Diagram of F-8 DFBW unreliability equations.

The conditional unreliabilities $Q(S|UTL, 2\overline{PC})$ and $Q(S|3\overline{HYD})$ are 1, i.e., the probability that the aircraft will be lost if both primary hydraulic systems fail is 1. In this study, however, these have been set to 0 since this is a failure mode which would be present in the basic aircraft before addition of the electronic flight-control system, and thus should not be charged to it. The other three conditional unreliabilities must be solved by the repeated application of the basic equation for the rest of the elements for the particular state of the hydraulic system.

The reason for computing unreliability instead of reliability can now be seen. The first term will be the conditional unreliability of the system with all elements good, which will be a very small number, multiplied by the probability that all are good, which will be a number very near 1. The last terms will be the conditional unreliability with elements failed, which will approach or be equal to 1, times the probabilities of these events, which will be very small. The arrangement will be very balanced numerically. If reliability had been used, the equation would have been the sum of the products of numbers very close to 1 and the products of very small numbers. This situation would be very difficult to handle without special precautions.

The next element is the generators. A typical equation is

$$Q(S|3HYD) = Q(S|3HYD, GEN)P(GEN) + Q(S|3HYD, \overline{GEN})P(\overline{GEN})$$

In this case, there is only one generator and thus there are only two events: the generator is good and the generator is bad. There are two other generator equations for the other two states of the hydraulic system.

The third element is the battery. The batteries are not involved if the generator is good. A typical equation is thus

$$\begin{aligned} Q(S|3HYD, \overline{GEN}) = {} & Q(S|3HYD, \overline{GEN}, 3BAT)P(3BAT) \\ & + Q(S|3HYD, \overline{GEN}, 2BAT, \overline{BAT})P(2BAT, \overline{BAT}) \\ & + Q(S|3HYD, \overline{GEN}, BAT, 2\overline{BAT})P(BAT, 2\overline{BAT}) \\ & + Q(S|3HYD, \overline{GEN}, 3\overline{BAT})P(3\overline{BAT}) \end{aligned}$$

At this point, it should be obvious how cumbersome the notation and the equations themselves can become. The conditional probability $Q(S|3HYD, \overline{GEN}, 3BAT)$ is assumed to be equal to $Q(S|3HYD, GEN)$, and does not have

to be computed twice. The term $Q(S|3HYD, \overline{GEN}, 3\overline{BAT})$ is 1, i.e., the system fails if it loses all dc power. All other conditional unreliabilities must be computed.

There are two other battery equations for the other two states of the hydraulic system. The events for the case where one hydraulic system is bad must be rearranged somewhat. There is now a distinction between a battery failure in the same channel as the failed hydraulic system or a battery failure in a different channel. If the battery fails in the same channel as the hydraulic failure, the state of the system will be the same as if only the battery had failed. The hydraulics in that channel are now not relevant since the electrical power in that channel has failed. If a battery fails in a channel with good hydraulics, it is assumed that the entire system has failed, since there is no automatic reconfiguration to single-channel operation for mixed hydraulic and electrical failures. The system can be reconfigured manually as will be discussed in Section 7. This distinction between battery-failure channels is shown in Figure 10a by the subscripts.

In the case where only one hydraulic system is working, the entire system has been reduced to a single-channel system, and thus only one battery is involved. The state of the other two batteries is of no consequence. The rest of the diagram was constructed in a similar fashion. At most levels there will be conditional unreliabilities of 1 corresponding to failures on that level that would cause total system failure. Other conditional unreliabilities must be computed from the failure rates of the remaining levels. Eventually, at or near the bottom of the diagram there will be zeros, which means that, within the assumptions of this model, there are sufficient elements working to guarantee the success of the system.

The equations for the probability of loss of the primary digital mode were formed as a subset of the total set of equations. To obtain them, one sets the conditional unreliabilities to unity at all points in the system equation where the system will revert to the bypass system.

SECTION 4

COMPUTER PROGRAM TO CALCULATE CONTROL-SYSTEM UNRELIABILITY

A computer program was written to compute the unreliability equations developed in Section 3. The program is organized in a modular fashion that duplicates the structure of equations defined by the probability model for the flight-control system. Failure rates for the calculations are stored in a separate data file to facilitate revisions without disturbing the computing program. These failure rates are summarized in Section 5 (Table 5).

The program provides for varying flight-time and failure rates in order to test the sensitivity of system unreliability (Q_{system}) to the duration of the mission and uncertainties in failure-rate estimates. Program output is formatted to tabulate the unreliability in each state of the model. This permits the user to trace critical failure paths that contribute to overall system unreliability. A modification of the total system model calculates the probability that the primary digital flight-control system will fail and cause reversion to the bypass system.

Application of Computer Program to Unreliability Equations

The unreliability model for the flight-control system is constructed from probability state equations containing sums and products of the probability states of each system element as described in the discussion of Eq. (2) (Section 3). The general expression is a particular case of Bayes' theorem, which is derived from the product laws of probability.[8] The basic equation is repeated here in the form

$$Q(S) = \sum_{i=1}^{n} P(A_i)Q(S|A_i) \qquad (4)$$

where

S = overall system unsuccessful state

$Q(S)$ = probability of system failure

A_i = various mutually exclusive and exhaustive states of the system elements

$P(A_i)$ = a priori probability that A_i will occur

$Q(S|A_i)$ = a posteriori probability of S given that A_i occurs

Applying the general equation we get

$$Q(S) = Q(S|A_1)P(A_1) + Q(S|A_2)P(A_2) + Q(S|A_3)P(A_3) + \cdots + Q(S|A_n)P(A_n) \quad (5)$$

The a priori terms may be calculated directly. For example, in a triplex voting system where two out of three elements are required for system success:

$P(A_1) = R_A^3$ All elements OK

$P(A_2) = 3R_A^2Q_A$ One element failed

$P(A_3) = 3R_AQ_A^2$ Two elements failed

$P(A_4) = Q_A^3$ All three elements failed

R_A and Q_A are, respectively, the reliability and unreliability of element A. In the general case

$$R_i = e^{-\lambda_i t} \quad (6)$$

and

$$Q_i = 1 - R_i \quad (7)$$

where λ_i is the constant hazard failure rate of the i^{th} element. The a posteriori (conditional) terms must be derived from additional equations.

This leads to a structure of equations whereby the probability of the top-level event—system failure—is calculated by a main program,

and conditional probabilities are calculated by nested subroutines called by the main program. Conditional probabilities for each equation in the hierarchy are then computed by further equations. The process continues until the conditional probabilities for all subsystem states have been accounted for. A set of equations organized in this manner may be visualized by observing Figure 11. This structure allows the program to be written "top-down", whereas the computations must be performed "bottom-up". The subroutine calling procedures automatically perform all of the necessary bookkeeping necessary to perform this transformation.

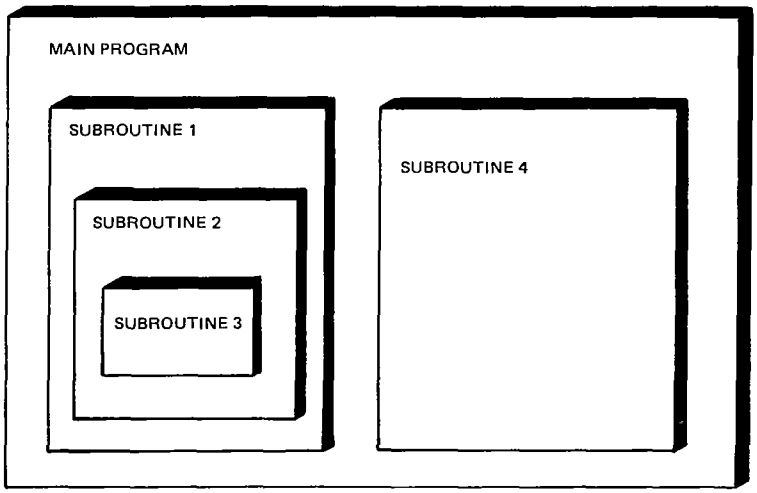


Figure 11. General program organization.

Organization of the Computer Program

The structure of the probability model covers a large number of the unique subsystem states that could potentially necessitate separate probability equations. This situation is saved by the fact that many system states are equivalent as far as the remaining elements are concerned, or can be defined in terms of the system totally failing or succeeding. In the case of equivalent states, one subroutine called by several equations can compute the desired probability. Where a state may be defined as leading directly to overall flight-system success or failure, we may input a conditional probability, $Q(S|A_i)$, of 0 or 1, as applicable.

Application of the general expression may be illustrated by the following example, which also highlights the modular organization of the probability equations. The top-level event, Q(S), failure of flight-control system, is identified by the reliability model as a function of the states of system elements. The first-level equation (refer to the discussion of Eq. (3) in Section 3) represents the analysis of the hydraulic system states, as defined in Table 4.

Table 4. Definition of hydraulic system states.

State	Mnemonic	Description
A_1	3 HYD	All hydraulic systems OK
A_2	2 HYD, 1 $\overline{\text{HYD}}$	Two hydraulic systems OK, one failed
A_3	PC, $\overline{\text{PC}}$, $\overline{\text{UTL}}$	One primary system OK, one primary system failed, utility system failed
A_4	UTL, 2 $\overline{\text{PC}}$	Utility system OK, primary systems failed
A_5	3 $\overline{\text{HYD}}$	All hydraulic systems failed

Nomenclature of Subroutines

Each subroutine computes the probability relationship for a unique system state, and is labeled by a mnemonic to facilitate program tracing and relating outputs to specific equations. The system for naming the subroutines is illustrated by the following example.

The probability of system failure is calculated in accordance with a hierarchy of equations, with those pertaining to the hydraulic systems considered first. The top-level event, total system failure, Q(S), is computed by Eq. (5) in a subroutine labeled "QSYSTEM". The first term in the equation, $Q(S|A_1)$, is the conditional unreliability of the system given that three hydraulic systems are not failed. Its value depends on the following two states:

(1) B_1: Three hydraulics OK, generator OK.

(2) B_2: Three hydraulics OK, generator failed.

Thus

$$Q(S|A_1) = Q(S|B_1)P(B_1) + Q(S|B_2)P(B_2) \qquad (8)$$

The subroutine computing this relationship is labeled "Q3HYD", and it is nested within "QSYSTEM", which calls it to obtain the value of $Q(S|A_1)$.

Equation (8) contains two conditional probability terms. These, in turn, are computed by nested subroutines as follows:

(1) $Q(S|B_1)$ is computed by "Q3HGEN".

(2) $Q(S|B_2)$ is computed "Q3HGEN_".*

The pattern is then continued until all states of the system have been exhausted and all conditional probabilities have been computed.

Subroutines are nested for efficient program execution to minimize computer search time. However, two special non-nested subroutines are provided to cover the following general cases:

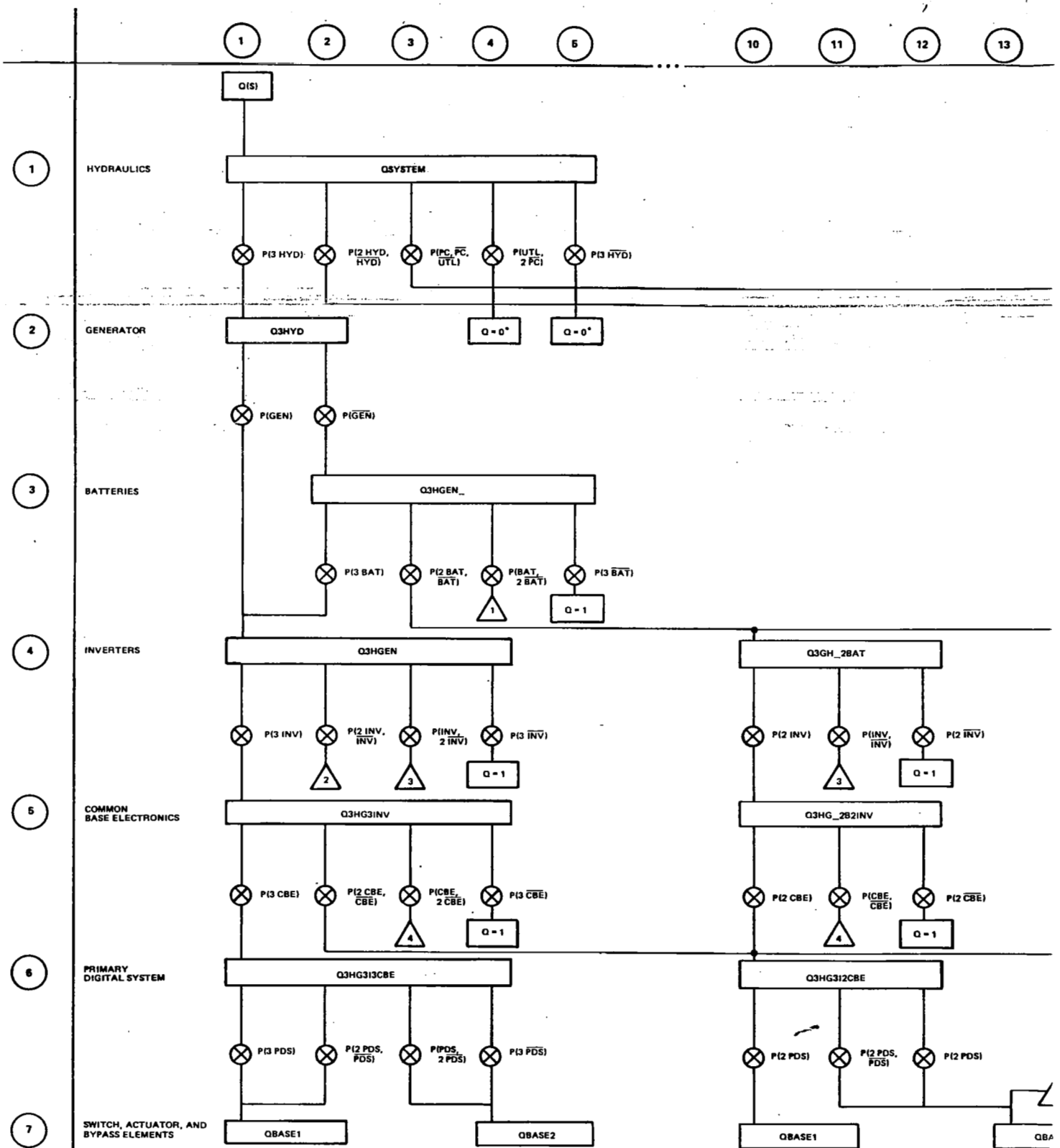
(1) "QBASE1" computes the unreliability of switch and actuation elements when the primary digital system is used (triplex or dual), or the primary digital system is not used and bypass is dual.

(2) "QBASE2" computes the unreliability of switch and actuation elements when the primary digital system is not used and bypass is triplex.

Figure 12 illustrates the flow of calculations through the computer program and corresponds directly to the equation diagram in Figure 10a. The system states are identified by a 19 × 27 matrix, and the conditional probabilities are tabulated with respect to the same coordinates. This tabulation is labeled "QS MATRIX" on the computer printout. The QS MATRIX may then be superimposed on an equation diagram and be used to trace critical failure paths for the flight-control system.

---

* The formatting ability of the computer precludes use of a bar over the symbol (e.g., $\overline{A}$) to indicate "not A" or "failure of element A", as in standard reliability terminology. Therefore, an underscore following the symbol is used to indicate "$\overline{GEN}$" (failure of the generator).



*LOSS OF AIRCRAFT DUE TO COMPLETE HYDRAULIC FAILURE NOT ALLOCATED TO ELECTRONIC FLIGHT-CONTROL SYSTEM.

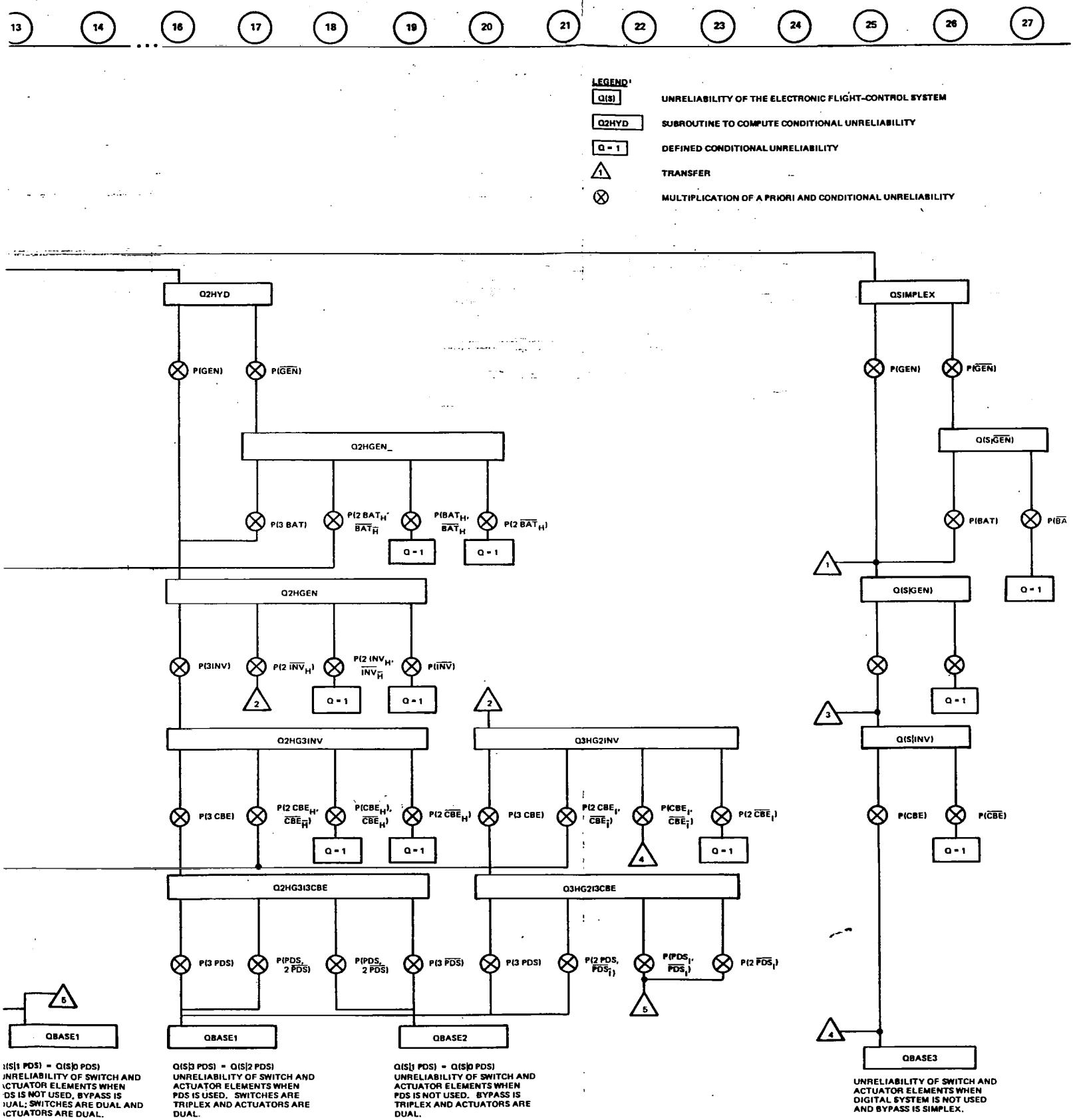


Figure 12. F-8 DFBW unreliabilit equations and compute program.

Probability that the Flight-Control System will Revert to the Computer Bypass System

The probability that the flight-control system will revert to the computer bypass system (CBS) is a subset of the overall probability model. A modified program was made by inserting unity at all points where the system would use the CBS. The following examples illustrate how such modifications are made to perform the desired calculations:

(1) If one primary hydraulic system and the utility hydraulic system fail, the electronic logic will reconfigure the flight-control system into a simplex string of elements operating on one channel through the bypass system. Therefore, by definition, the primary digital system (PDS) is not available and the conditional unreliability for this event is 1.

To incorporate this change into the program, subroutine "QSYSTEM" is modified as follows:

(a) Subroutine "QSIMPLEX" is deleted as it no longer applies.

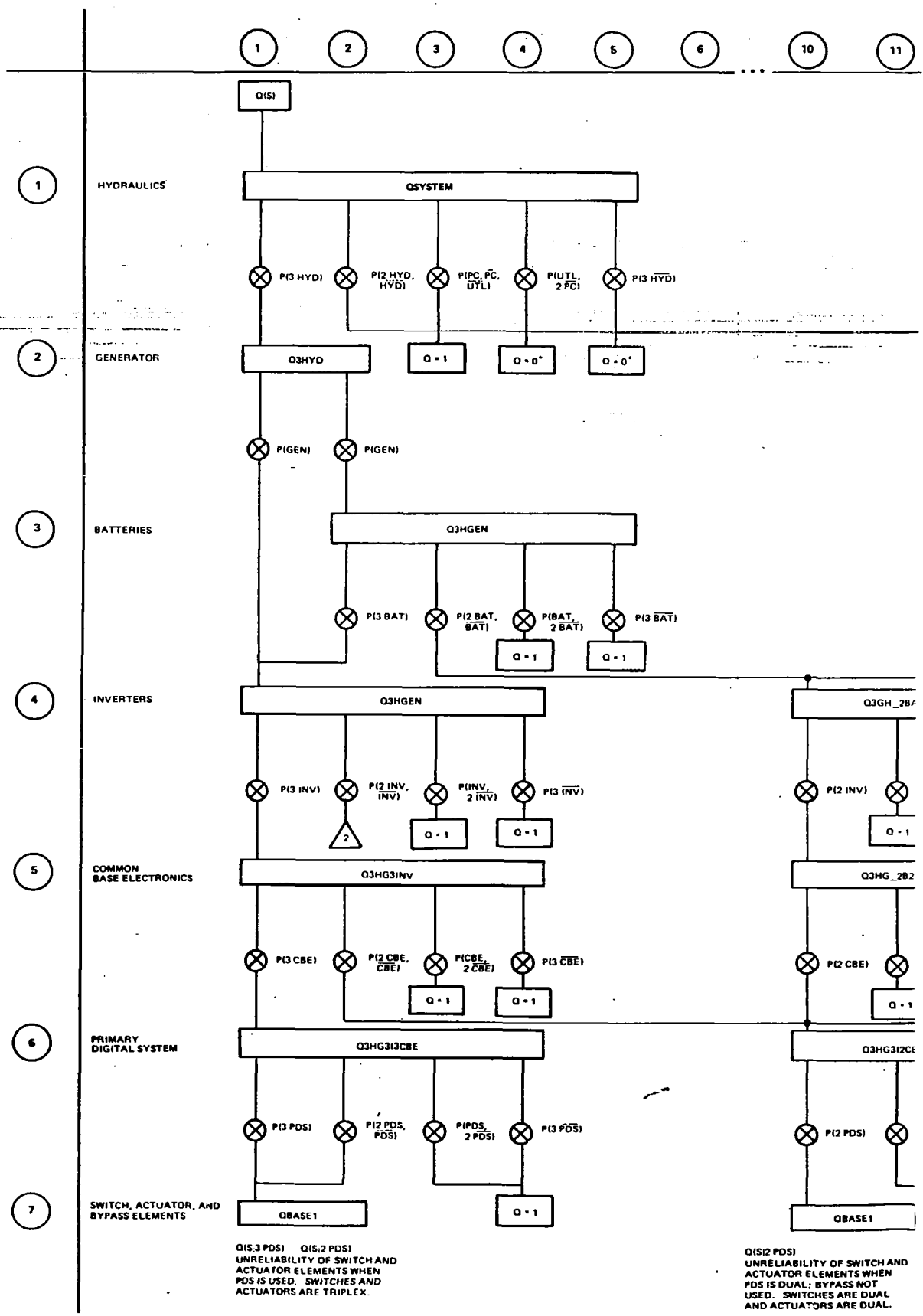
(b) The conditional unreliability $Q(S|PC, \overline{PC}, \overline{UTL})$ is set equal to 1.

It should be noted that the conditional unreliabilities $Q(S|UTL, 2\overline{PC})$ and $Q(S|3\overline{HYD})$ are 0 as in the overall system model because these states represent total hydraulic failure whether or not the electronic flight-control system is used and, therefore, the incremental unreliability is not allocated to the DFBW system.

(2) In row 7 of Figure 12, there are three boxes labeled "QBASE2" and they represent reconfiguration of the flight-control system to bypass. Since these states indicate that the PDS is not used, the conditional unreliabilities are set equal to 1, and subroutine QBASE2 is deleted from the program.

(3) Transfers in other subroutines that indicate reconfiguration to manual mode are set equal to 1. Examples are $Q(S|INV, 2\overline{INV})$ in "Q3HGEN" and $Q(S|CBE, \overline{CBE})$ in "Q3HG_2B2INV".

Figure 13 is a revised diagram of the equations used to compute the probability that the flight-control system will revert to CBS.



*LOSS OF AIRCRAFT DUE TO COMPLETE HYDRAULIC FAILURE NOT ALLOCATED TO ELECTRONIC FLIGHT-CONTROL SYSTEM.

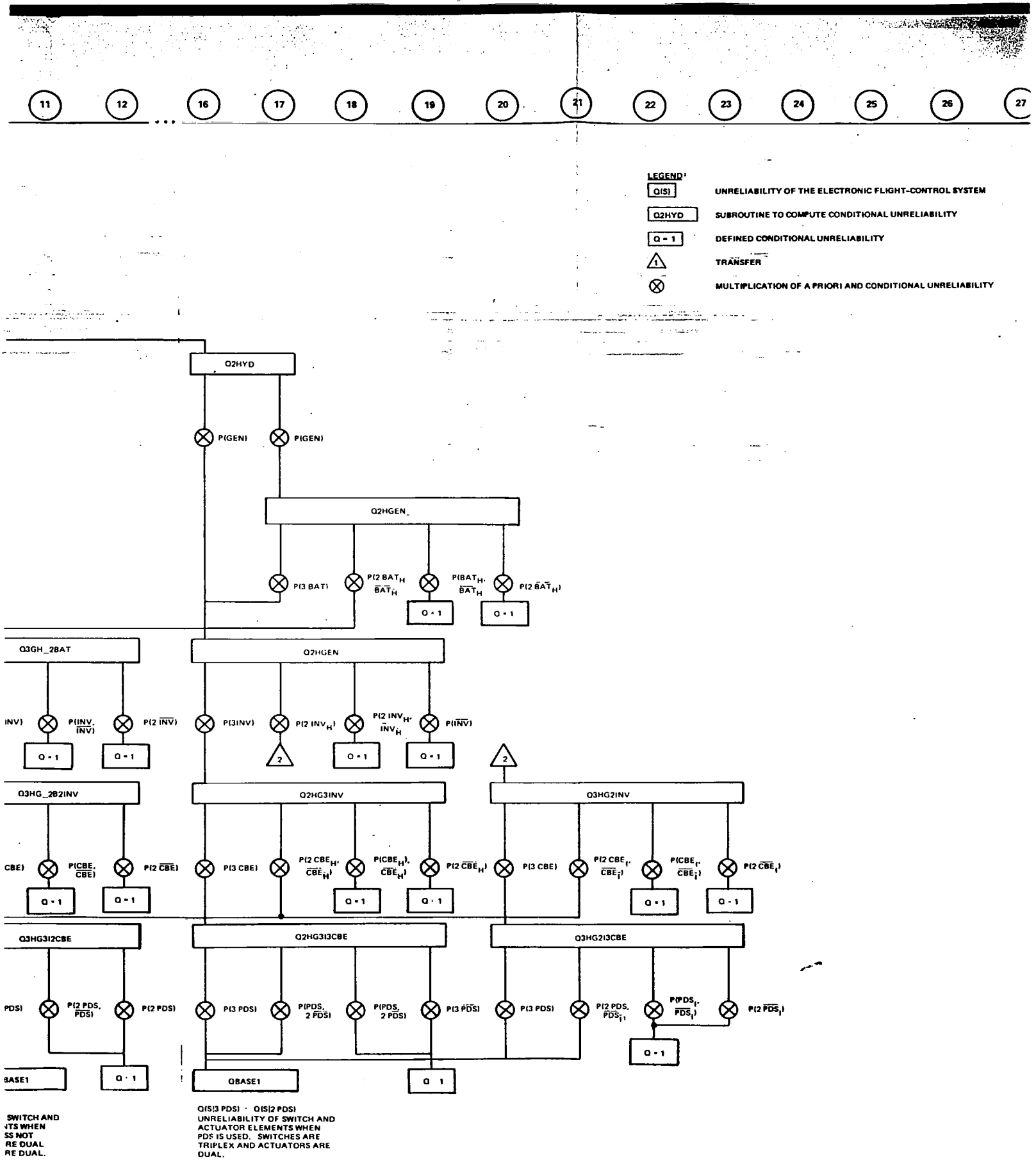


Figure 13. Unreliability equation and computer program f digital control mode.

SECTION 5

DEVELOPMENT OF BASIC COMPONENT FAILURE RATES

Operational failure rates for system components have been derived from operational experience with the system, data collected by principal users of such equipment, and standard references developed for reliability prediction. In all cases it is assumed that each component has been used beyond the "infant mortality" range, where many design, quality, or manufacturing faults may cause premature failure. It is also assumed that each component is within its useful life. Therefore, failures will be randomly distributed within the time interval under consideration, and the failure rate will be constant. Table 5 summarizes the subsystem failure rates used to compute the unreliability of the flight-control system.

Table 5. Summary of failure rates used to compute unreliability of flight-control system (failures per 10^6 hours).

Subsystem	Failure Rate	Subsystem	Failure Rate
Hydraulics	125.6	Left Pitch Switch	12.2
Generator	597.6	Left Pitch Actuator	192.3
Batteries	356.8	Roll Backup System	108.3
Inverters	45.7	Right Roll Switch	12.2
Common BASE Electronics	39.3	Right Roll Actuator	192.3
Primary Digital System	1522.0	Left Roll Switch	21.1
Pitch Backup System	108.3	Left Roll Actuator	192.3
Right Pitch Switch	12.2	Yaw Backup System	108.2
Right Pitch Actuator	192.3	Yaw Switch	12.2
		Yaw Actuator	192.3

Reliability Prediction Methods

The criterion governing the selection of a data source and the method of computation is that each failure rate shall be consistent with the others in terms of estimate uncertainty and the level of detail with which the mathematical model of system unreliability was constructed. For example, if detailed operational records for a piece of equipment were available over a significant time interval covering many part-hours of operation, then the failure rate was computed from the recorded data. However, if these conditions were not met, then the failure rate was computed from standard references by the parts-count technique given in MIL-HDBK-217C. No attempt was made to estimate component failure rates by detailed part-stress analysis, as this level of information is not available and it would be inconsistent with the detail of the system unreliability model.

Operational Failure Data

If the failure rate for a component is to be calculated from operational experience, then the following apply:

(1) It is assumed that failures are random and that there is an exponential distribution of failure times.

(2) Two-sided 90-percent confidence limits are computed as follows:*

$$\text{Lower Confidence Limit (LCL)} = \frac{\chi^2_{(\alpha/2,2r)}}{2T}$$

$$\text{Upper Confidence Limit (UCL)} = \frac{\chi^2_{(1-(\alpha/2),2r+2)}}{2T}$$

where

r = number of failures and determines the degrees of freedom used to find chi-square (χ^2)

$\alpha/2$ = 5^{th} percentile coordinate used to determine the χ^2 value at the lower confidence limit

$1-\alpha/2$ = 95^{th} percentile coordinate used to determine the χ^2 value at the upper confidence limit

T = total number of component part hours

---

* Failure rates in NPRD-1 (Reference 9) are tabulated with 60-percent confidence limits, whereas predecessor documents, the RADC Notebooks (Reference 10), used 90-percent confidence limits.

(3) A special case occurs when the part under evaluation has had zero failures. In this instance, the failure point estimate is calculated as a function of total part-hours, and the χ^2 value is obtained from the upper single-sided 60-percent confidence level at two degrees of freedom. No confidence limits are given for failure rates calculated in this manner.

Predicted Failure Data

Electronic Equipment. - The parts-count reliability prediction of MIL-HDBK-217C was used unless otherwise notes. This method is applicable when a detailed parts list including part stresses is not available. The general expression for equipment failure rate is

$$\lambda_{EQUIP} = \sum_{i=1}^{n} N_i (\lambda_G \pi_Q)_i \qquad (9)$$

for a given equipment environment, where

λ_{EQUIP} = total equipment failure rate (failures $\times 10^{-6}$/h)

λ_G = generic failure rate for the i^{th} generic part (failures $\times 10^{-6}$/h)

π_Q = quality factor for the i^{th} generic part

N_i = quantity of the i^{th} generic part

n = number of generic-part categories

It has been assumed that the generic failure rates are based on an uninhabited airborne fighter (A_{UF}) environment unless otherwise noted.

Quality factors are based on:

(1) Microelectronics (integrated circuits and op amps) procured to quality level B-1 as defined in Table 2.1.5-1 of MIL-HDBK-217C.

(2) Discrete semiconductors procured to JAN quality.

(3) Capacitors, resistors, coils, and transformers of established reliability types (ER) procured to MIL specification quality.

Nonelectronic Equipment. - Failure rates for nonelectronic equipment are generally based on the information contained in NPRD-1, Nonelectronic Parts Reliability Data (Reference 9), unless otherwise noted. NPRD-1 is the result of an extensive data collection program to summarize failure-rate data by component type and environment. The data are presented in terms of failure rate per million part-hours or part-cycles, with upper and lower statistical confidence limits. Background information such as number of records, part-hours, or part-cycles is also tabulated.

Computation of Subsystem Failure Rates

The probability equations for calculating system unreliability are based on a hierarchy of subsystem dependencies which have been previously described. The details of calculating the subsystem failure rates are discussed as follows using the same order of dependencies.

Hydraulic System Failure Rate

An analysis of failures pertaining to the primary hydraulic systems on all F-8 aircraft in service during calendar year 1978 was performed. The details of such failures are set forth in a special maintenance data report (Reference 11) submitted by the Navy Maintenance Support Office (NAMSO), Mechanicsburg, Pennsylvania.

The data indicate that there were 293 failures associated with the primary hydraulic systems, and they occurred as shown in Table 6. One in-flight abort was due to internal failure of the system pressure transmitter, and the other was due to a loose hydraulic hose. No further details are available about the symptoms surrounding the latter failure, but evidently the pilot was aware of the malfunction and turned the system off while in flight.

The 11 preflight aborts as well as the 280 other faults should not be counted against the in-flight failure rate of the hydraulic system since, by definition, system reliability is the probability that a system will not fail given that it was in a nonfailed state at the start. Therefore, we get (refer to section on operational failure data)

Total flight hours for all F-8 aircraft in 1978 = 7,962

Table 6. Primary hydraulic system unscheduled maintenance actions for all F-8 aircraft, 1978.

When Discovered	No.	Percent
Before flight (abort)	11	3.75
In-flight (abort)	2	0.68
All other	280	95.56
Total	293	99.99

Because there are two primary hydraulic systems per aircraft

$$\text{Total part-hours} = 7{,}962 \times 2 = 15{,}924$$

$$\lambda = \frac{2}{15{,}924} = 125.6 \times 10^{-6}/\text{h}$$

$$\text{LCL} = \frac{\chi^2_{(0.05,4)}}{31{,}848} = 22.3 \times 10^{-6}/\text{h}$$

$$\text{UCL} = \frac{\chi^2_{(0.95,6)}}{31{,}848} = 395.6 \times 10^{-6}/\text{h}$$

Information pertaining to the utility hydraulic system was not included in the NAMSO report. However, a conservative assumption is to use the same failure rates as those calculated above. Therefore, the 125.6×10^{-6}/h value for λ_{HYD} has been entered in both Table 5 and the computer program. Further research into other studies on similar aircraft indicates that these values are consistent with experience; Reference 12 cites a failure rate of 140×10^{-6}/h for typical fighter aircraft hydraulic systems.

Generator Failure Rate

The research aircraft was retrofitted with a 30-volt 300-ampere generator (MS 90332-1) and a voltage regulator (MS 19071-2). The failure rates for each, in accordance with Reference 9, are 489.649 and 107.924 per 10^6 hours, respectively.* Since both pieces of equipment must function in order to produce dc power, λ_{GEN} is the sum, or 597.6×10^{-6}/h.

Battery Failure Rate

Figure 14 is a partial schematic of the dc power circuit. It can be shown that the battery function depends upon the parts listed in Table 7. The major contribution to the failure rate in the dc power circuit is from the battery.

According to the manufacturer, battery failure is a function of the breakdown of the barrier material between the cells, which is a wear-out phenomenon. A battery of this type would have to have three cells fail simultaneously in order to fail to perform the required function. If it were properly serviced and checked out prior to each flight, then, according to the manufacturer, the probability of battery failure in-flight would be extremely remote. A company reliability study yielding a mean time between failure (MTBF) of 6897 hours ($\lambda = 145 \times 10^{-6}$) was cited.

NPRD-1 (Reference 9) gives a failure rate for nickel cadmium batteries in an airborne environment that is based on 8.055×10^6 operating hours. The NPRD-1 value is more conservative and was used in the system calculations.** The failure rates for the other components were obtained from MIL-HDBK-217C.

---

* The 90-percent confidence limits (failures per 10^6 hours) for the generator are 455.506 and 525.491. For the voltage regulator, they are 98.761 and 117.648. See Reference 10.

** 90-percent confidence limits are 338.079 and 359.855 failures per 10^6 hours. See Reference 10.

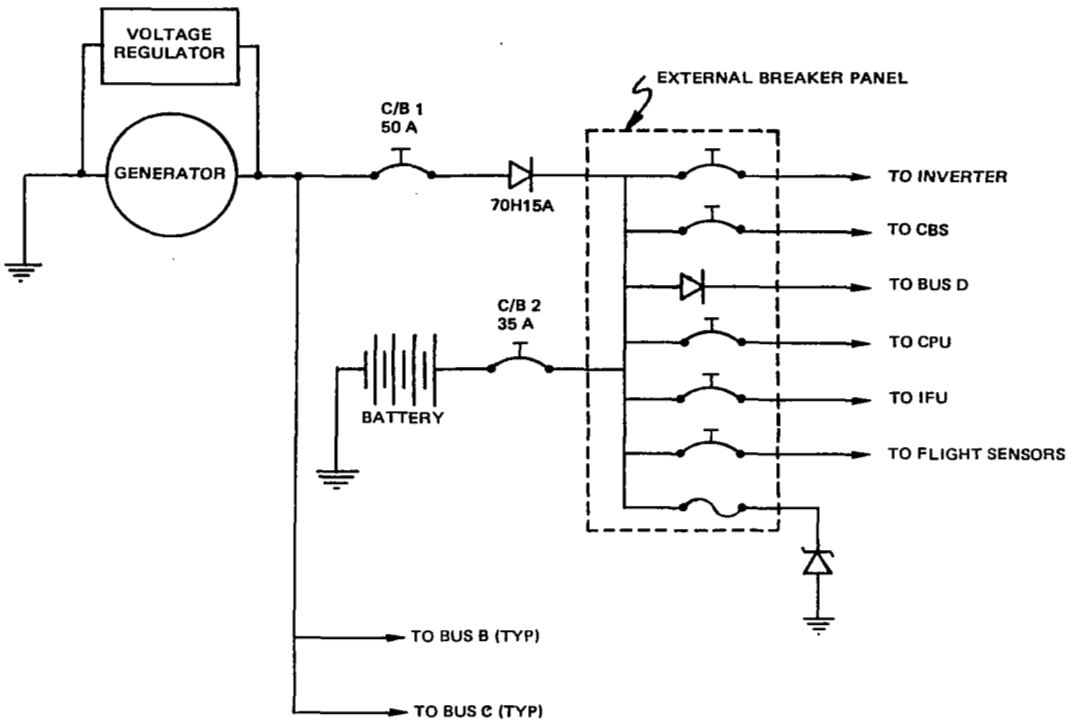


Figure 14. Partial schematic of dc power circuit.

Table 7. Calculation of battery circuit failure rate (λ_{BAT}).

Part	Failure Rate ($\times 10^{-6}$/h)
Battery	348.852
C/B 1 (50 A)	2.0
Power isolation diode (70H15A)	2.7
C/B 2 (35 A)	2.0
Fuse	0.1
Zener diode	1.1
Total	356.752

Inverters

The F-8 is equipped with three inverters, and a parts-count reliability prediction using the criteria of Eq. (9) yields an estimated failure rate of 45.7×10^{-6}/h. Salient factors that affect the failure rate estimate are:

(1) Components are of standard commercial quality screened by incoming inspection per MIL-STD-105D.

(2) A comprehensive in-process inspection and test program is utilized.

(3) The power supply is encapsulated and hermetically sealed to meet the environmental requirements of MIL-STD-810C and MIL-E-5400P, Class 2, including: altitude (to a vacuum), high temperature (+100°C), low temperature (-54°C), temperature shock (-54 to +100°C), temperature-altitude (-54 to 71°C, 0 to 70,000 ft), sunshine, rain, humidity, fungus, salt fog, dust, explosion, immersion, acceleration, vibration, and shock.

(4) The power supply is designed to assure adequate heat transfer when used under system parameters.

The manufacturer advertises a typical MTBF for this series of dc-to-400-Hz inverters of 55,000 hours ($\lambda = 18.18 \times 10^{-6}$/h), and submitted a report detailing the computations to arrive at this figure. The calculations were based on MIL-HDBK-217 (original edition dated 8 August 1962). A recalculation by CSDL in accordance with MIL-HDBK-217C (9 April 1979), assuming part stress levels set forth in the manufacturer's report and the uninhabited airborne fighter (A_{UF}) environment, gives an estimated failure rate of 29.025×10^{-6}/h (MTBF = 34,453 hours).

It is felt that the difference between the failure-rate calculations for this report and the vendor's catalog numbers are due to substantial revisions in the methods of MIL-HDBK-217 and refinements in the mathematical models of the MIL handbook. In order to be consistent with other failure rates, the value obtained by parts-count prediction, which is a more conservative number, was selected for the system calculations. For similar reasons, the parts-count method was used to derive the predicted failure rates for the IFU power supplies (refer to Table 13).

Bypass and Servo Electronics (BASE) Failure Rates

The BASE units may be partitioned for reliability study purposes into logical elements consistent with the data flow between the computer bypass system (CBS), the digital computer system (DCS), and the secondary hydraulic servo actuators. Failure rates were computed by the parts-count method based on representative circuit diagrams, and the results were allocated to the subsystems as defined by the computer program. BASE functions are partitioned as follows:

(1) Interface with the digital control system.

(2) Common BASE electronics.

(3) Computer bypass systems for the pitch, roll, and yaw axes.

(4) PDS/CBS switches for each pitch, roll, and yaw control surface.

(5) Actuation of control surfaces including the nonelectronic portion of the hydraulic secondary servo actuators.

Failure rate of the BASE digital interface. - The predicted value is 50.0172×10^{-6}/h based upon the parts-count method of MIL-HDBK-217C using schematic diagrams provided by DFRC. The result has been allocated to the primary digital system (PDS) failure-rate calculation (refer to Table 12).

Failure rate of the BASE power-supply card. - Each channel of BASE has a power-supply section with a 28-Vdc input that provides ±15 and 5 Vdc output to other functions. For this study, the power supply is labeled common BASE electronics (CBE). The predicted failure rate based on the parts-count method of MIL-HDBK-217C is 34.3322×10^{-6}/h.

Failure rates of BASE pitch, roll, and yaw bypass systems. - The bypass receives inputs from the pilot's control stick, rudder pedals, manual trim commands, and wing-position analog and discrete signals. These signals are combined and processed for each axis. The processing network for each axis is labeled: pitch bypass system, roll bypass system, and yaw bypass system.

A predicted value of 87.7106×10^{-6}/h was derived based on the parts-count method of MIL-HDBK-217C using the manufacturer's drawings for the pitch function. The failure rates of the roll and yaw functions

are assumed to be the same based on similarity. Contributions to system unreliability from nonflight-critical functions such as trim or wing-position discrete signal processing are not included.

Failure rates of BASE PDS/CBS switches. - There are five solid-state PDS/CBS switches within the flight-control system to manage command paths for right pitch, left pitch, right roll, left roll, and yaw. The predicted failure rate for each switch based on the parts-count method of MIL-HDBK-217C is 12.2×10^{-6}/h.

Failure rates of BASE actuation functions. - There are five actuation systems within the BASE to command channel equalization and synchronization and middle-value logic (MVL) operation for the closed-loop servo drive. The failure rate of the mechanical components associated with the hydraulic secondary servo actuators is added to the failure rate of the electronic subsystems to derive a failure rate of each actuation function. These functions are identified as: right pitch actuation (RPA), left pitch actuation (LPA), right roll actuation (RRA), left roll actuation (LRA), and yaw actuation (YA). The predicted failure rate for each function is 158.9994×10^{-6}/h per MIL-HDBK-217C.

The failure rate for the hydraulic secondary actuator is based on DFRC data, which states

$$\text{Part-hours} \approx 3 \text{ channels/actuator} \times 5 \text{ actuators/system} \times 2000 \text{ h}$$

$$= 30 \times 10^{3} \text{ h}$$

One hard failure on a servo valve was recorded during ground test. Therefore

$$\lambda = \frac{1}{30 \times 10^{3}} = 33.3333 \times 10^{-6}/\text{h}$$

and 90-percent confidence limits are

$$\text{UCL} = 158.2 \times 10^{-6}/\text{h}$$

$$\text{LCL} = 1.7 \times 10^{-6}/\text{h}$$

The data is based on the period up to October 1978, which covers most of the operating experience on the system to date. Combining the two estimates, we get a predicted failure rate of 192.3327×10^{-6}/h for the actuation function.

The failure rate derived for the hydraulic secondary servo actuator was compared to values reported by other sources such as:

(1) RADC Reliability Notebook (RADC-TR-69-458, Section 2), [10] which gives failure rates in an airborne environment of:

Actuator, linear, hydraulic servo = 130.423×10^{-6}

Actuator, linear, hydraulic = 136.837×10^{-6}

(2) NASA Report CR-2609, Preliminary...Study for (F8 DFBW) by Secord and Vaughn (Reference 13), which cites a failure rate of 20.6×10^{-6}.

The values reported by these sources are within the computed confidence limits based on DFRC data. The F-8 hydraulic secondary servo actuator is a high-reliability component specifically designed for this flight-critical application, and it is capable of functioning with at least one of three channels operating. Therefore, the empirical failure rate was selected because it is consistent with the ground-rule preference for detailed operational records over standard references, and because the results do not disagree with failure rates obtained from other sources.

Comparison of calculated versus observed failure rates for BASE. - DFRC experience pertaining to BASE faults is presented in Table 8. Calculations of failure rates based on the DFRC data are set forth in Tables 9 and 10.

A summary of the calculated versus observed failure rates is given in Table 11. It can be seen that the observed values are considerably larger than the predicted values. Several factors may explain this:

(1) The actual F-8 hardware is an engineering prototype. Therefore, many failures can be expected due to design and manufacturing difficulties and so-called "infant mortality" or "burn-in" factors. With normal learning-curve experience, such failures can be predicted to diminish and, in fact, approximately 50 percent occurred before the first flight.

(2) None of the faults listed in Table 8 caused a total channel failure. It is possible that another reason for the difference between the observed and predicted values may lie with the definition of what constitutes a failure. A comprehensive failure-reporting and analysis system was not in place during the development of the BASE electronics prior to flight qualification.

Table 8. DFRC experience—BASE faults.*

	Number of Faults			Operating Hours as of 11 July 1978
	Computer Bypass Circuit	Voter Electronics	Servo Electronics	
Before first flight	3	0	5	—
Since first flight	3	5	2	—
Totals	6	5	7	—
Breakdown:				
Channel A	0	1	0	1,790
Channel B	3	2	4	1,881
Channel C	3	2	3	1,842

* None of the above faults caused total channel failure.

Table 9. Calculation of bypass-circuit failure rate based on DFRC data.

Box	Operating Hours	Part Hours (Operating Hours × 3)	Failures
A	1,790	5,370	0
B	1,881	5,643	3
C	1,842	5,526	3
Totals	5,513	16,539	6
Failure Rate = 6/16,539 = 362.8×10^{-6}/h			
LCL = 158.1×10^{-6}/h			
UCL = 716.5×10^{-6}/h			

Table 10. Calculation of voter and servo electronics failure rate based on DFRC data.

Box	Operating Hours	Part Hours (Operating Hours × 5)	Failures
A	1,790	8,950	1
B	1,881	9,405	6
C	1,842	9,210	5
Totals	5,513	27,565	12

Failure Rate = 12/27,565 = 435.3×10^{-6}/h

LCL = 250×10^{-6}/h

UCL = 751×10^{-6}/h

Table 11. Comparison of calculated versus observed BASE failure rates.

Summary of Values	Failure Rate ($\times 10^{-6}$/h)
Calculated:	
Digital interface	50.0
Common BASE electronics	39.3
Pitch, roll, and yaw bypass systems ($3 \times 87.7 \times 10^{-6}$/h)	263.1
Primary/bypass switches ($5 \times 12.2 \times 10^{-6}$/h)	61.0
MVS/servo actuators ($5 \times 159 \times 10^{-6}$/h)	795.0
Total	1,208.4 (MTBF = 828 h)
Observed:	
Bypass circuits ($3 \times 362.8 \times 10^{-6}$/h)	1,088.4
Voter and servo electronics ($5 \times 435.3 \times 10^{-6}$/h)	2,176.5
Total	3,264.9 (MTBF = 306 h)

Failure Rate of the Primary Digital System

The primary digital system (PDS) is comprised of three separate but identical channels as shown by the functional reliability diagram of Figure 15. Each channel contains a digital control computer, which is a general-purpose stored-program machine containing the control-law and system-redundancy management software.

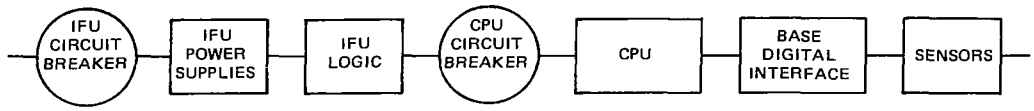


Figure 15. Functional reliability diagram of one channel of primary digital system.

The computer communicates with a specially designed dedicated interface unit (IFU) that processes and conditions its input and output signals. Each IFU channel contains three power supplies, which convert 28-Vdc prime aircraft power to voltages required by the IFU.

As previously noted, the digital interface circuits within each BASE channel are functionally included within the PDS, and their failure rate contributes to the estimated value of λ_{PDS}. The remaining contributions to the PDS failure rate are from the pilot's stick and pedal sensors and the circuit breakers in the central processing unit (CPU) and IFU bus. The above listed contributions to PDS failure rate are set forth in Table 12.

Table 12. Failure rate of primary digital system (PDS).

Part	Failure Rate ($\times 10^{-6}$/h)
IFU power supplies:	
±15 V, 1.0 A	55.2
5 V, 10 A	37.4
5 V, 2.5 A	35.3
IFU logic	650.3
CPU	689.7
Base digital interface circuits	50.0
Sensors	nil
Circuit breakers to CPU and IFU (2 at 2.0)	4.0
Total	1,521.9

Failure rate of IFU power supplies. - Each IFU channel contains three power supplies to convert the 28-Vdc aircraft power to voltages required by various elements within the IFU. Using the parts-count method of MIL-HDBK-217C, we get the values listed in Table 13. See the inverters section for a discussion of the factors pertaining to calculation of these failure rates.

Table 13. Failure rates of IFU power supplies.

Power Supply	Failure Rate ($\times 10^{-6}$/h)
±15 V, 1.0 A	55.156
5 V, 10 A	37.358
5 V, 2.5 A	35.256

Failure rate of IFU logic. - The IFU logic considered in the failure analysis is that required to implement only the direct mode of operation of the Digital Control System as shown in functional form in Figure 16. The failure rate, calculated in accordance with the parts-count method of MIL-HDBK-217B, is 650.3×10^{-6}/h.

Failure rate of CPU. - Eight flight computers have been used in conjunction with the F-8 DFBW program. These are the first units of that model in production. The goal in establishing a failure rate to be used for this reliability study was to obtain a "best estimate" of a projected value once the development problems have been resolved.

The computer is used in other applications as well. Accordingly, the manufacturer and users were contacted for assistance in establishing a reasonable estimate of the failure rate for a mature production unit. There have been numerous corrective action changes made by the manufacturer to improve the reliability of the production units. Not all of these actions were possible with the F-8 DFBW computers.

Based upon discussions with the manufacturer and users, a conservative MTBF of 1450 hours ($\lambda = 689.7 \times 10^{-6}$/h) was used in this study.

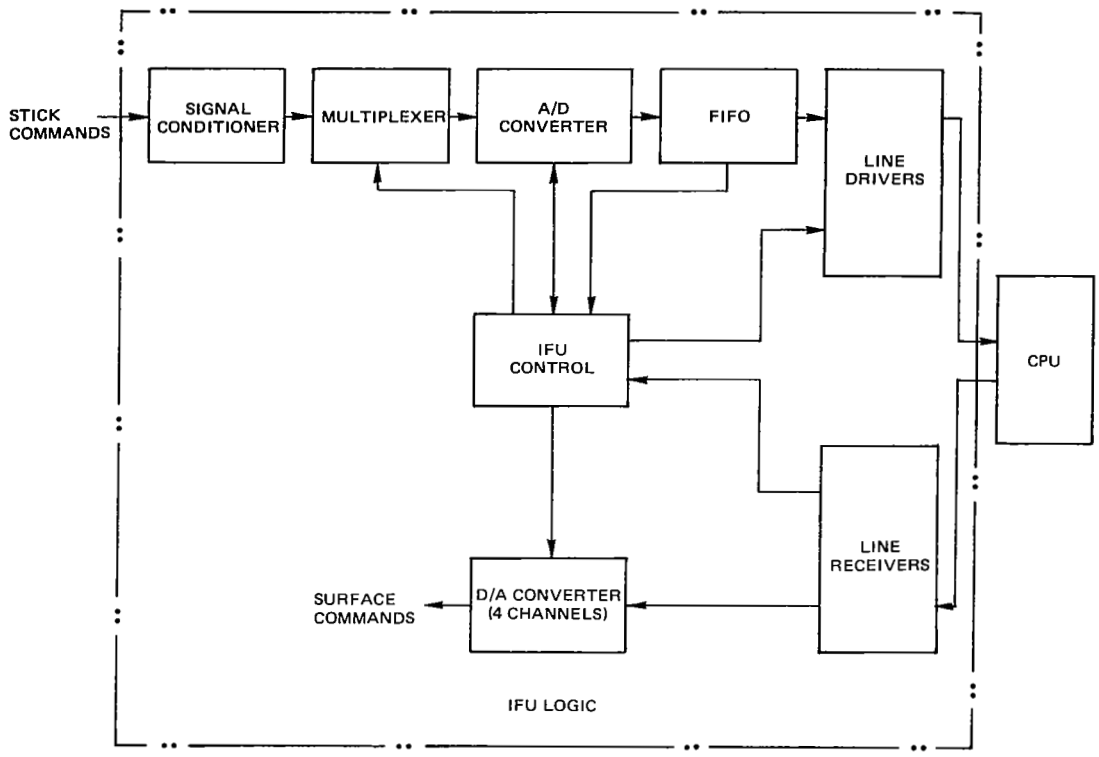


Figure 16. Functional diagram of the direct mode of the IFU logic.

Failure rate of sensors. - The stick and pedal sensors within each channel are interconnected according to the reliability diagram of Figure 17. The success paths in this configuration are:

(1) Pitch and roll (side stick).

(2) Pitch and roll (center stick).

(3) Pitch (center stick) and yaw.

(4) Pitch (side stick) and yaw.

Operational experience reported by users indicates that the failure rate of the sensor, which is also used on the F-111, is 20.6×10^{-6}/h with upper and lower 90-percent confidence limits of 3.7×10^{-6}/h and 48.9×10^{-6}/h. Using

$$\lambda_{sensor} = 20.6 \times 10^{-6}/h$$

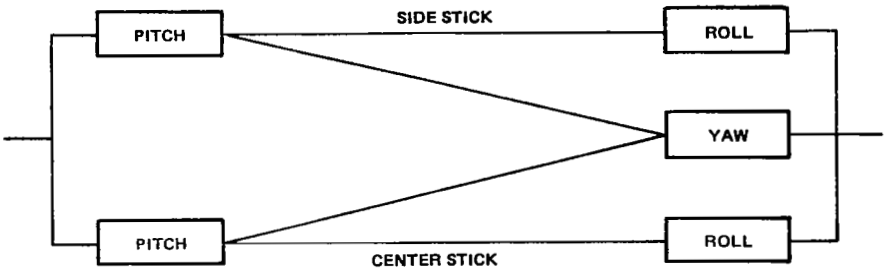


Figure 17. Reliability diagram of stick and pedal sensors (each channel).

and assuming t = 1 hour, the unreliability (Q) of this configuration is 424×10^{-12}. Therefore, the failure rate of the sensor array is significantly less than the failure rates of other PDS elements, and it is entered as "nil" in Table 12.

Failure rates of miscellaneous elements. - In Figure 15, two circuit breakers are shown in series with the IFU and CPU. These failure rates have been added to Table 12.

SECTION 6

RESULTS OF THE RANDOM-FAILURE ANALYSIS

The estimates of component failure rates developed in Section 5 can now be inserted into the analysis model and corresponding program described in Sections 3 and 4. The first half of this section gives the resulting unreliability estimates for the total system and for the primary digital control mode. These results are given as a function of time for the total probability of failure over that time period, the average failure rate, and the instantaneous failure rate. The sensitivity of the system unreliabilities to uncertainty in estimates of input reliabilities of the individual elements is also given.

The second half of this section interprets the results in terms of how the final number was generated as a summation of all potential failure combinations. Of particular interest is the identification of the failure combinations that make the largest contribution to the total system unreliability. The potential utility of this technique to analyze system modifications is illustrated.

System Unreliability as a Function of Time

A typical mission for the F-8 experimental aircraft is approximately 1 hour, and the F-8 fuel capacity limits flights to less than 2 hours. However, missions of up to 10 hours were considered as they could permit an estimate of unreliability for a similar digital flight-control system installed in a longer range aircraft (e.g., transport or bomber) or the same system performing in an F-8 flight with air-to-air refueling.

The primary task of this study was to determine the probability of loss of the F-8 aircraft due to a failure of the flight-control system. The results are presented in Table 14 and Figure 18, and indicate a system unreliability of approximately 6.4×10^{-8} for a nominal 1-hour flight. The results are plotted in a semilog format as the values of Q(t) increase by three decades to 6.8×10^{-6} for a 10-hour flight. The average failure rate for the system is set forth in Table 15.

Table 14. System unreliability as a function of duration of flight.

t (h)	Q_{system}
0.5	1.6055×10^{-8}
1.0	6.4463×10^{-8}
1.5	1.4550×10^{-7}
2.0	2.5948×10^{-7}
3.0	5.8752×10^{-7}
5.0	1.6525×10^{-6}
10.0	6.8161×10^{-6}

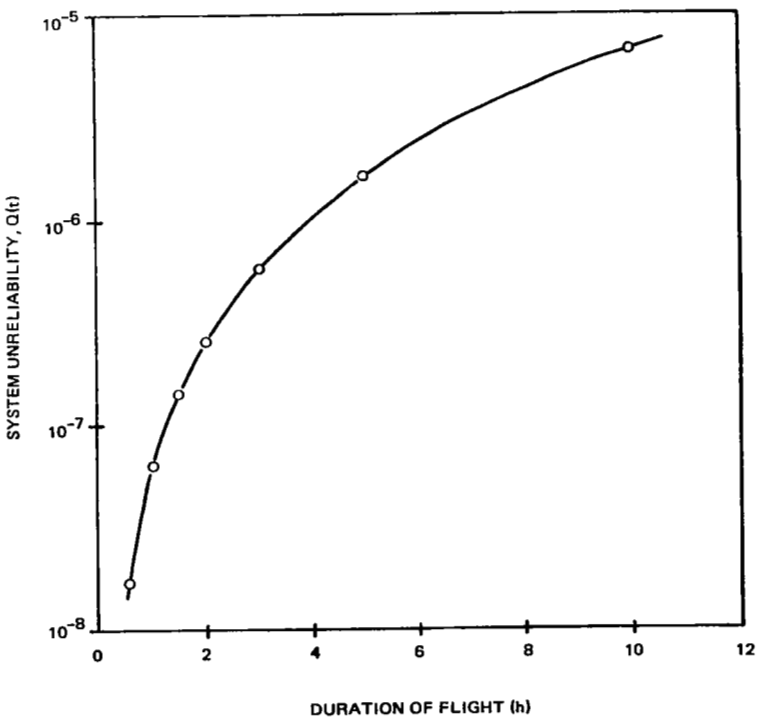


Figure 18. System unreliability versus duration of flight.

Table 15. Average failure rate of digital flight-control system as a function of duration of flight (Q_{system}/t).

t (h)	Average System Failure Rate ($\times 10^{-9}$/h)
0.5	32.1
1.0	64.4
1.5	97.0
2.0	129.7
3.0	195.8
5.0	330.5
10.0	681.6

The second task was to determine the probability of failure of the primary digital flight-control mode. These results are displayed in Table 16 and Figure 19, which show an unreliability of 7.8×10^{-6} at 1 hour to 7.6×10^{-4} at 10 hours. Again, because the values of Q(t) increase by three decades, the data is plotted in a semilog format. The average failure rate is tabulated in Table 17.

Table 16. Unreliability of digital flight-control mode as a function of duration of flight.

t (h)	$Q_{digital\ mode}$
0.5	1.058×10^{-6}
1.0	7.825×10^{-6}
1.5	1.758×10^{-5}
2.0	3.122×10^{-5}
3.0	7.009×10^{-5}
5.0	1.938×10^{-4}
10.0	7.661×10^{-4}

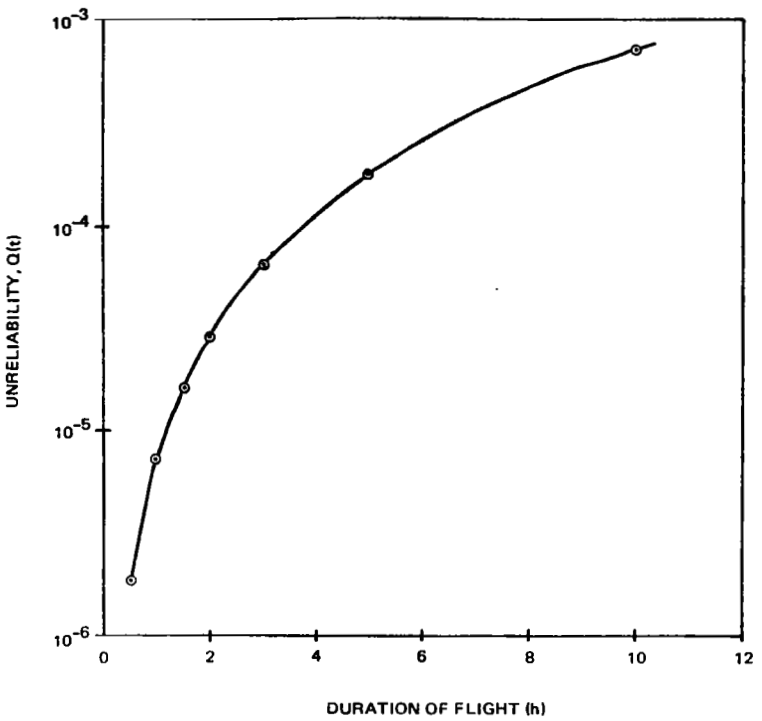


Figure 19. Unreliability of digital mode versus duration of flight.

Table 17. Average failure rate of digital flight-control mode ($Q_{digital\ mode}/t$).

t (h)	Average Failure Rate Digital Mode ($\times 10^{-6}$/h)
0.5	3.92
1.0	7.83
1.5	11.7
2.0	15.6
3.0	23.4
5.0	38.8
10.0	76.6

System Hazard Rate Function

For the exponential distribution, the conditional probability that a device will fail within a range of time values depends only upon range and not upon position. This is a peculiar and significant property of the exponential distribution, and applies to no other distribution. For this reason, the exponential distribution is a constant hazard distribution in which λ is a random variate representing the times to failure of the device.

A system comprised of redundant, cross-linked, and voting elements does not exhibit a constant failure rate or hazard function. Its failure rate at any given time increases as various members within it fail or are voted out of the system.

If we represent the failure rate by $Z(t)$, then it can be calculated by*

$$Z(t) = \frac{1}{R(t)} \frac{dQ(t)}{dt} \tag{10}$$

From the definition of the derivative

$$\frac{dQ(t)}{dt} = \lim_{\Delta t \to 0} \frac{Q(t + \Delta t) - Q(t)}{\Delta t} \tag{11}$$

$R(t)$, the probability that the system has survived up to time t, is approximately equal to 1 and, therefore, has a negligible effect upon the calculations.

Thus $Z(t)$ may be empirically estimated from the values of $Q(t)$. For the flight-control system, the values are set forth in Table 18, and indicate a tenfold increase in the hazard rate from 0.130×10^{-6} at t = 1 hour to 1.40×10^{-6} at t = 10 hours. An increment of Δt = 0.01 hour was found suitable for appropriate accuracy. Similarly, Table 19 lists the hazard rates for the primary digital mode and indicates an increase from 15.7×10^{-6}/h at t = 1 hour to 151×10^{-6}/h at t = 10 hours. An increment of Δt = 0.01 hour was also used.

---

* Reference 8, p. 271.

Table 18. Instantaneous failure rates of flight-control system.

t (h)	Z(t) ($\times 10^{-6}$/h)
0.5	0.065
1.0	0.130
1.5	0.196
2.0	0.262
3.0	0.396
5.0	0.670
10.0	1.400

Table 19. Instantaneous failure rates of primary digital system.

t (h)	Z(t) ($\times 10^{-6}$/h)
0.5	7.91
1.0	15.71
1.5	23.50
2.0	31.30
3.0	46.60
5.0	77.00
10.0	151.00

Sensitivity of System Unreliability to Failure-Rate Estimates

Failure rates used in the probability calculations were best estimates based on operational experience or standard references in accordance with the criteria set forth in Section 5.

An analysis of the sensitivity of the final answer, Q_{system}, to uncertainties in failure-rate estimates indicates that only three elements have a significant effect: hydraulics, inverters, and common BASE electronics (CBE). The results are presented in Table 20, where the failure rates for each subsystem were individually doubled and halved to determine the effect upon the calculation of Q_{system}. The sensitivity of the unreliability of the primary digital mode is shown in Table 21. It can be seen from this table that the failure rate is almost completely dominated by the primary digital system itself, as would be expected. The other elements have very little influence.

Table 20. Sensitivity of flight-control system unreliability to uncertainty of failure-rate estimates ($Q_{system} = 6.446 \times 10^{-8}$ at t = 1 h; all failure rates nominal).

Subsystem	Q_{system} With Each $\lambda_{subsystem}$ Adjusted as Shown	
	Failure Rate ×2 ($\times 10^{-8}$)	Failure Rate $\times\frac{1}{2}$ ($\times 10^{-8}$)
Hydraulics	12.87	3.23
Generator	6.46	6.44
Batteries	6.46	6.44
Inverters	9.90	4.72
CBE	9.42	4.96
Primary digital system	6.46	6.44
Bypass systems (pitch, roll, yaw)	6.46	6.44
PDS/CBS switches	6.45	6.45
Actuation systems	6.47	6.44

Table 21. Sensitivity of primary digital system unreliability to uncertainty of failure-rate estimates (Q_{system} = 7.825×10^{-6} at t = 1 h; all failure rates nominal).

Subsystem	Q_{system} With Each $\lambda_{subsystem}$ Adjusted as Shown	
	Failure Rate ×2 ($\times 10^{-6}$)	Failure Rate $\times\frac{1}{2}$ ($\times 10^{-6}$)
Hydraulics	7.98	7.77
Generator	7.83	7.82
Batteries	7.83	7.82
Inverters	8.30	7.59
CBE	8.24	7.62
Primary digital system	29.32	2.24
Bypass systems (pitch, roll, yaw)	7.82	7.82
PDS/CBS switches	7.82	7.82
Actuation systems	7.82	7.82

Use of Analysis Technique to Increase Understanding of System Failure Characteristics

The analysis technique and the associated computer program can be used as a powerful tool to increase the understanding of the system's failure characteristics. To facilitate easy interpretation, the intermediate results that lead to the final number are printed in a format that corresponds to the diagram of the failure equations. A typical output is shown in Figure 20. This listing corresponds to the summary of the equation diagram in Figure 21, including the row and column designations. This diagram is a condensed version of the diagram given in Figure 10.

The top number in each row is the unreliability of the system for that particular state up to that level. The numbers below each top number in the first six rows are the individual terms that are summed to get the top number. Each is the product of the probability of the particular event defining the state of the elements at that level and the conditional unreliabilities of the system for that particular

state of the system. Figure 22 shows the first six levels with lines drawn in from the reliability diagram to show how the numbers are interrelated. Careful study of this diagram can reveal much about the nature of the failure process and the contributions made by each part.

Identification of the Largest Contributors to Unreliability

The failure modes that make the largest contribution to the system unreliability can be easily traced from the computer output as shown by the highlights in Figure 23. At the first level, hydraulics, the middle term is more than two orders of magnitude larger than the other two terms. This means that the greatest system unreliability will be when one hydraulic system is failed. System unreliability for this state is given in column 16. The fact that the unreliability did not change much between the generator level and the inverter level means that neither generator failures nor battery failures make a significant contribution to the system unreliability. This result is to be expected, since the batteries in parallel with the generator form, in effect, an additional level of redundancy above triplex, and thus will have a much lower contribution than the elements that are only triplex.

The terms in the inverter equation starting in column 16 show significant contributions from both the first and third terms. The following equation for common BASE electronics is dominated by the third term. Thus, the whole system unreliability is dominated by the two terms in column 18 in the inverter and common BASE electronic equations.

The major contributors (99 percent) to the unreliability due to random failures are thus two failure combinations. These are the failure of one hydraulic system and the failure of either an inverter or a common BASE electronics element in one of the other two channels. A major reason why these modes are most critical is that virtually all of a channel is dependent on these power sources so that a failure of one is equivalent to multiple failures of actuation and sensor elements.

The criticality of the electrical power supplies was recognized, and thus the system was designed to automatically switch to the one remaining good channel after the second failure. Also, the standard procedure is to disengage actuator channels after hydraulic failures. When the second hydraulic system fails and is disengaged, and the good system is engaged manually, there is no total failure of the system.

		1	2	3	4	5	6	7	8	10	11	12	13
HYDRAULICS	1	6.45E-08 2.12E-10	6.42E-08	6.11E-12									
GENERATOR	2	2.12E-10 2.11E-10	7.41E-13		0.00E+00								
BATTERIES	3		1.24E-09 2.11E-10	9.11E-10	7.38E-11	4.54E-11							
INVERTERS	4	2.11E-10 9.82E-11	1.12E-10	9.25E-13	9.54E-14					8.51E-07 8.36E-07	1.35E-08	2.09E-09	
COMMON BASE ELEC	5	9.82E-11 2.56E-13	9.74E-11	5.02E-13	6.07E-14					8.36E-07 8.26E-07	8.52E-09	1.54E-09	
PRIMARY DIGITAL SYS	6	2.56E-13 1.23E-14	5.64E-17	2.44E-13	1.24E-16					8.26E-07 1.67E-07	6.59E-07	5.02E-10	
PITCH BYPASS	7				3.52E-08 1.78E-14	1.95E-13	3.52E-08	1.27E-12					2.17E-04 3.03E-07
RT PITCH SW	8	1.24E-14			1.78E-14			6.01E-10		1.67E-07			3.03E-07
RT PITCH ACT	9	1.23E-14			1.78E-14			2.72E-12		1.57E-07			2.93E-07
LEFT PITCH SW	10		1.11E-07			1.11E-07			2.45E-05		4.09E-04		
LEFT PITCH ACT	11		1.11E-07			1.11E-07			1.11E-07		3.85E-04		
ROLL BYPASS	12				5.43E-15								1.36E-07
RT ROLL SW	13	1.38E-21			1.92E-21			9.28E-17		6.84E-11			1.05E-10
RT ROLL ACT	14	1.38E-21			1.91E-21			4.20E-19		6.43E-11			9.83E-11
LEFT ROLL SW	15		1.24E-14			1.72E-14			3.79E-12		1.67E-07		
LEFT ROLL ACT	16		1.23E-14			1.71E-14			1.71E-14		1.57E-07		
YAW BYPASS	17						1.54E-07						
YAW SW	18			1.11E-07			1.11E-07		2.45E-05			4.09E-04	
YAW ACT	19			1.11E-07			1.11E-07		1.11E-07			3.85E-04	
		1	2	3	4	5	6	7	8	10	11	12	13

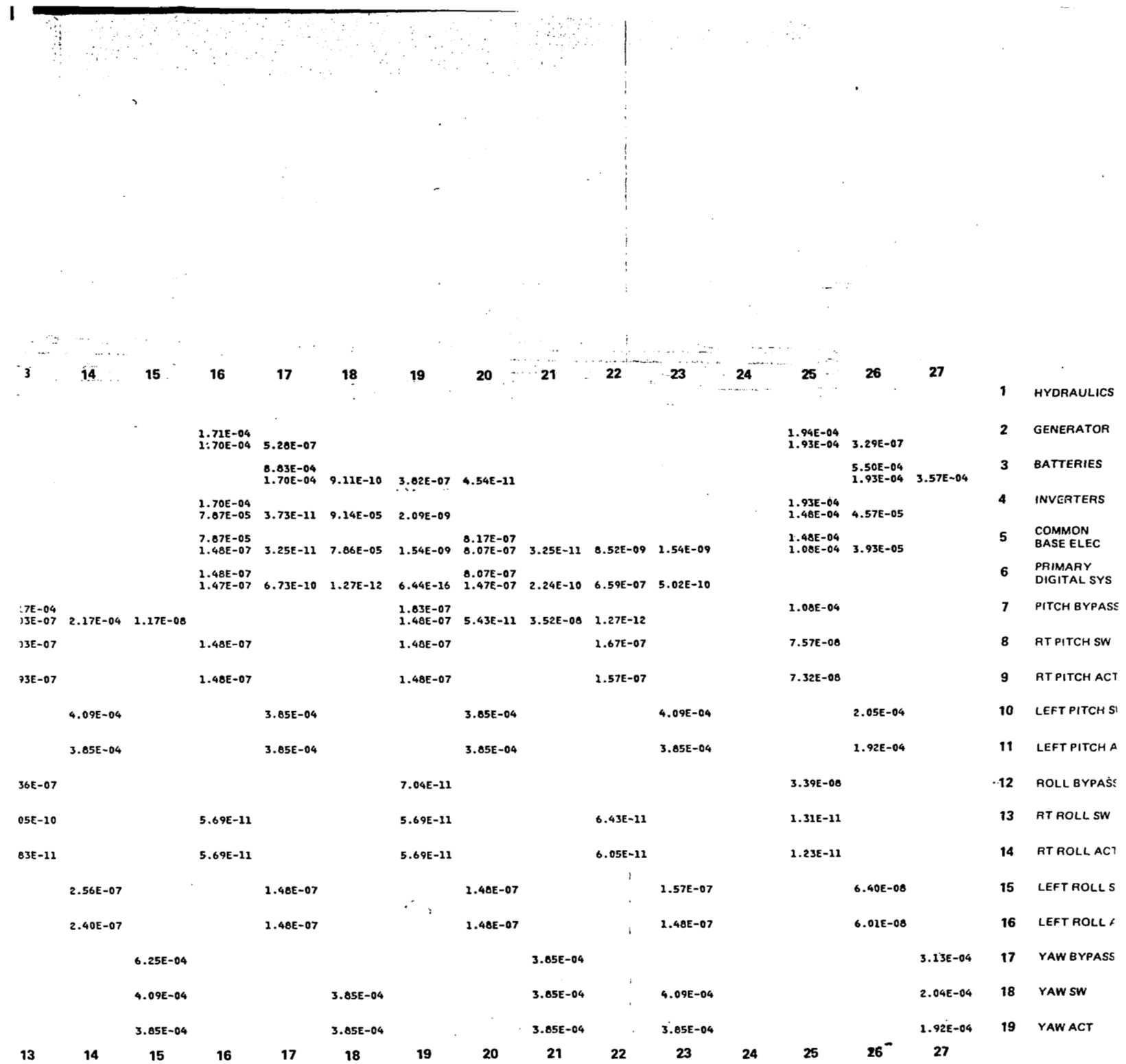
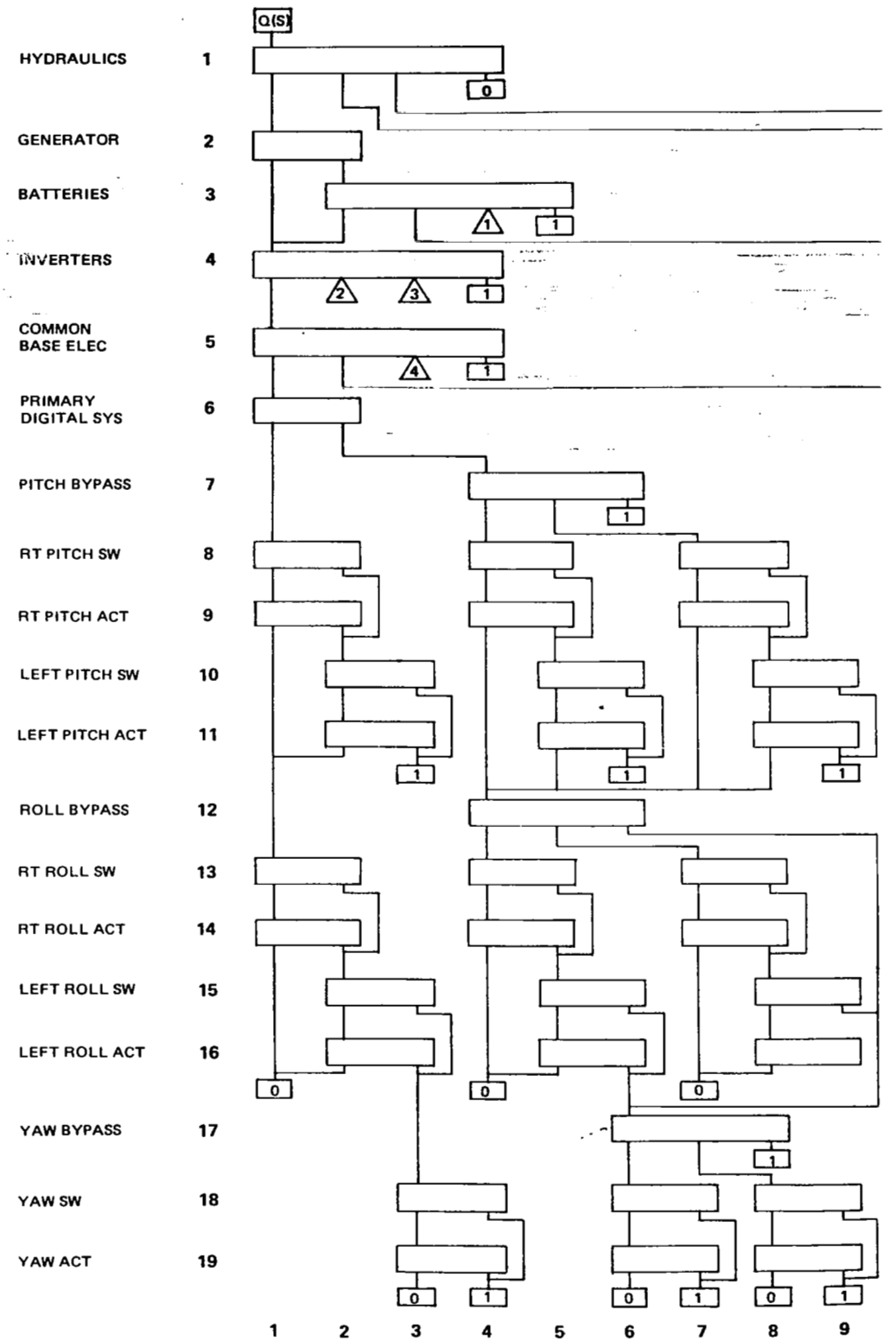


Figure 20. Computer analysis results for F-8 unreliability.


HYDRAULICS 1
GENERATOR 2
BATTERIES 3
INVERTERS 4
COMMON BASE ELEC 5
PRIMARY DIGITAL SYS 6
PITCH BYPASS 7
RT PITCH SW 8
RT PITCH ACT 9
LEFT PITCH SW 10
LEFT PITCH ACT 11
ROLL BYPASS 12
RT ROLL SW 13
RT ROLL ACT 14
LEFT ROLL SW 15
LEFT ROLL ACT 16
YAW BYPASS 17
YAW SW 18
YAW ACT 19
Q(S)
1 2 3 4 5 6 7 8 9

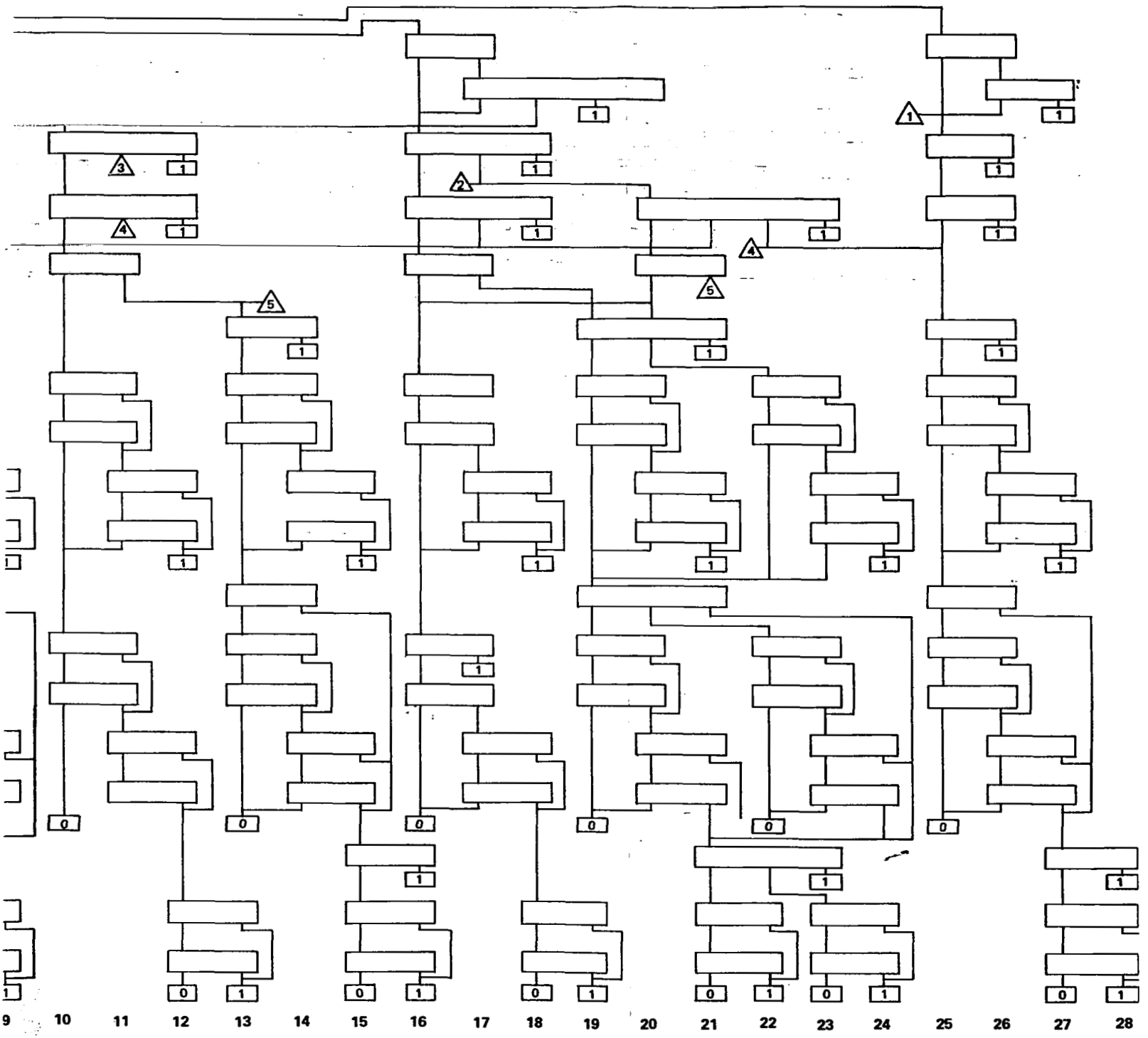


Figure 21. Reduced diagram of F-8 DFB unreliability equations.

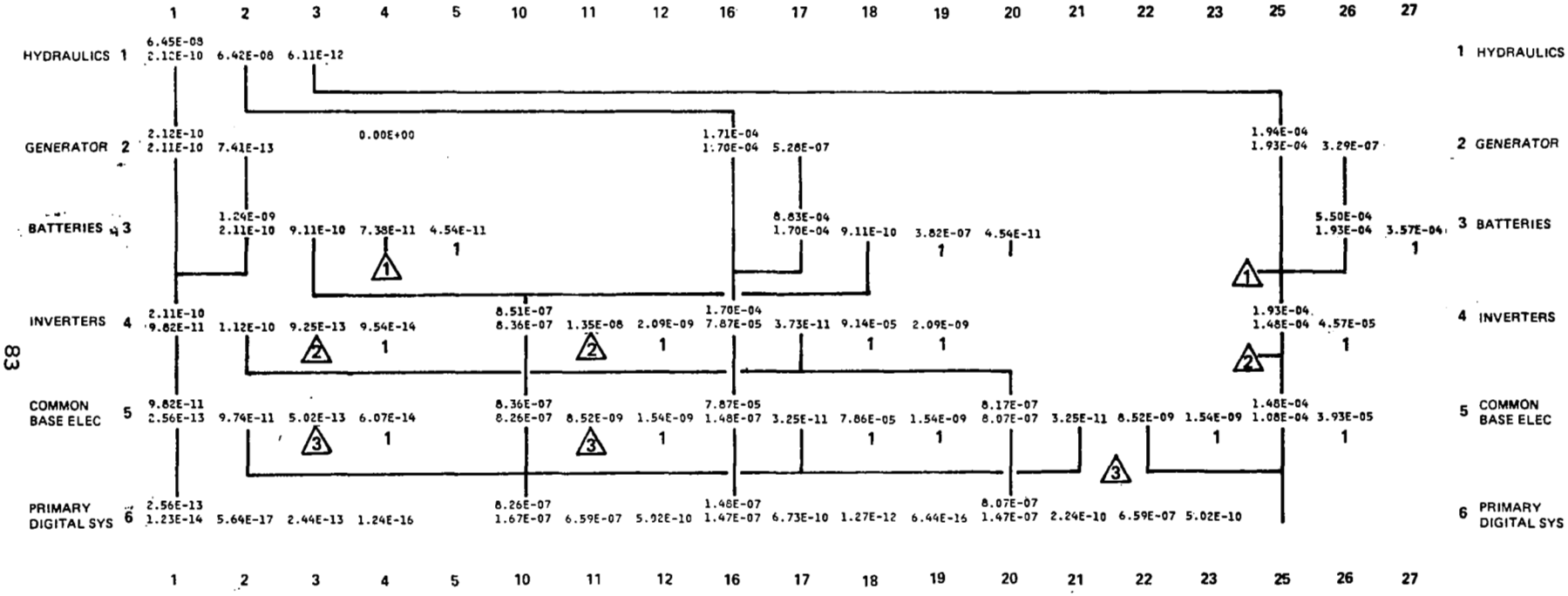


Figure 22. Results from top levels of program.

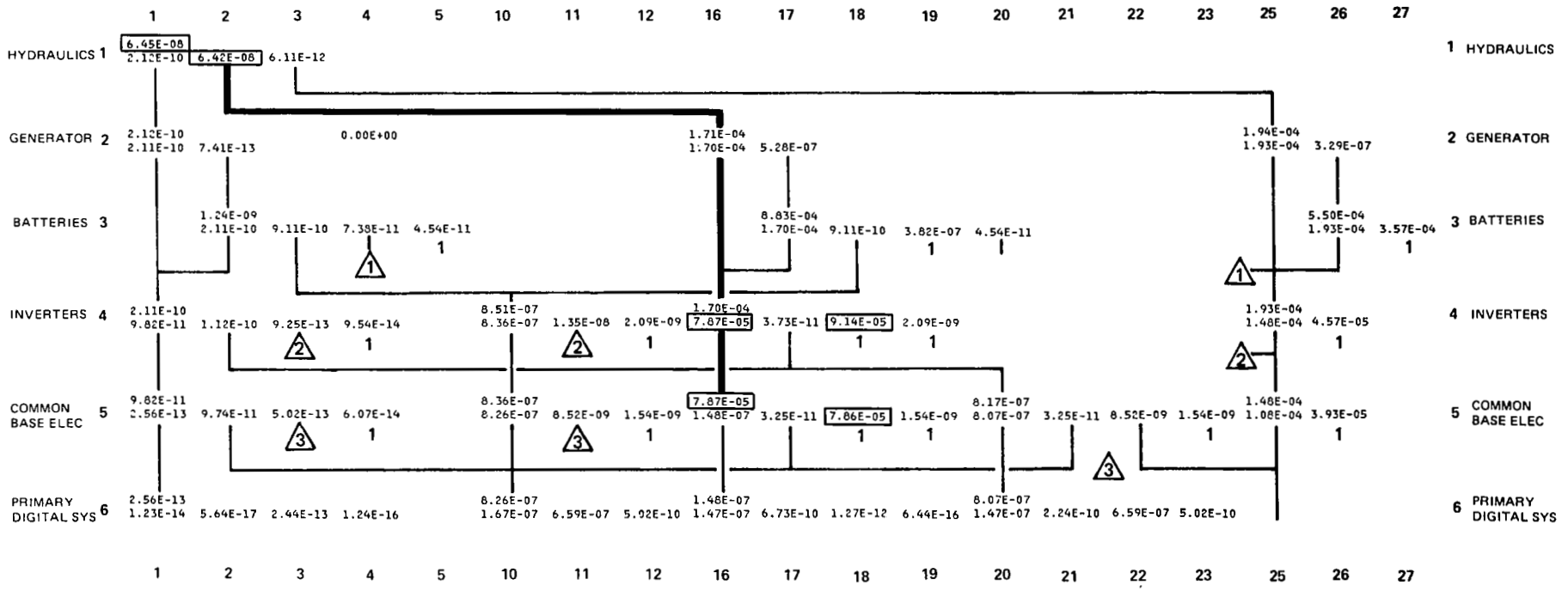


Figure 23. Critical failure path.

The dominant failure modes result from a hybrid situation which is not automatically accounted for in the system. A discrete signal indicating hydraulic system failure is not wired into the system. Thus, when one hydraulic system and one electrical power supply fail, the midvalue-select and comparison monitors for Δp will still be operating in two channels and can vote out the good channel or shut the entire axis off.

The analysis here is conservative. The actual unreliability will be less for two reasons. First, if there is a failure in any complete axis, and it is not at a critical time, the pilot could manually switch to the remaining good channel. Second, the Δp comparison thresholds are set wide such that the system is likely to continue to operate normally on the one good channel without the Δp becoming large enough to cause a comparison failure for cruise flight. This situation was demonstrated with an informal experiment using the F-8 "iron bird". On the other hand, the Δp threshold could contribute to a situation in which the system continues to operate normally, and the pilot will not be forced to switch to manual mode on the one good channel. The system could then disengage if large surface motion is commanded at a time when a manual recovery would be impossible.

Possible System Modifications and Analysis of a Modified System

The system could be modified relatively easily to significantly reduce these two largest failure modes. This system would be modified by including a discrete signal in each channel indicating the health of the corresponding hydraulic system. This discrete would be included in the logic the same way as it is for electrical power monitoring discretes, and would thus cause the system to automatically revert to single channel with any combination of two electrical or hydraulic power failures.

The equation diagram for the first four levels would be modified as shown in Figure 24. The results for the modified system are shown in Figure 25. The predicted unreliability due to random failures in a 1-hour flight is reduced by two orders of magnitude from the previously tabulated values. The most significant contributors to the total unreliability can again be traced by inspection of Figure 25. The primary failure modes and their percent contributions are given as follows:

(1) Failure of one inverter and failure in one of the two channels with good inverters of both a primary digital system and a pitch bypass system.
Contribution: 40 percent.

(2) Failure of a common BASE electronics and failure in one of the two channels with good CBE of both a primary digital system and a pitch bypass system.

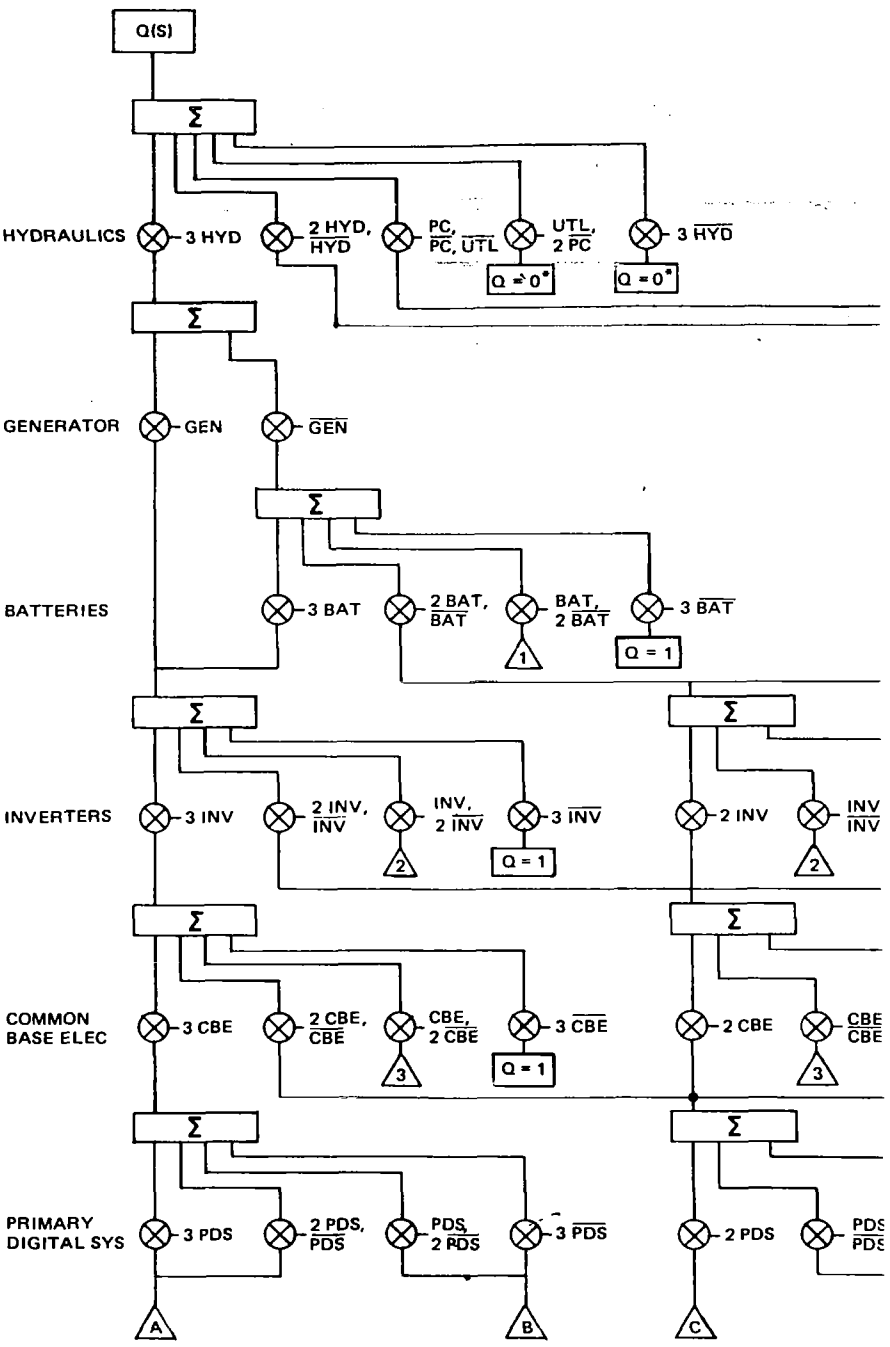
Contribution: 35 percent.

(3) Failure of one hydraulic system and failure of one of two remaining actuation channels for both left and right elevators.

Contribution: 23 percent.

It can be seen that the failure modes are now more balanced. There is no one element or combination of failures that dominates the unreliability. No further simple modification of the system was found that would significantly improve the system.

The unreliability of such a modified system as a function of time was computed. The results are given in Table 22 and Figure 26. The most significant characteristic is the rapid growth in the failure rate. The system is likely to be able to meet the Federal Aviation Regulations (FAR) that a catastrophe due to system failure is extremely improbable (Part 25.1309, where "extremely improbable" is interpreted as a failure rate of 10^{-9} per hour) for a 1-hour flight. However, the failure rate at the end of a 10-hour flight is two orders of magnitude larger. This rise in failure rate is typical of a fixed-configuration triplex system. As time passes and components fail, the probability that an additional failure will cause complete system failure is greatly increased. It can thus be seen that a basic change in the system design would be necessary to meet the requirements for commercial operation. One possible change would be to add additional levels of redundancy, so that even though the unreliability increased with time, the system would be so much more reliable that it would still meet the FAR requirements at the end of the required time period. Another possibility, which might produce a more efficient total design, is a reconfigurable system that would replace failed elements from a pool of spare elements. The rate of growth of the unreliability could thus be essentially eliminated.



*LOSS OF AIRCRAFT DUE TO COMPLETE HYDRAULIC FAILURE NOT ALLOCATED TO ELECTRONIC FLIGHT-CONTROL SYSTEM.

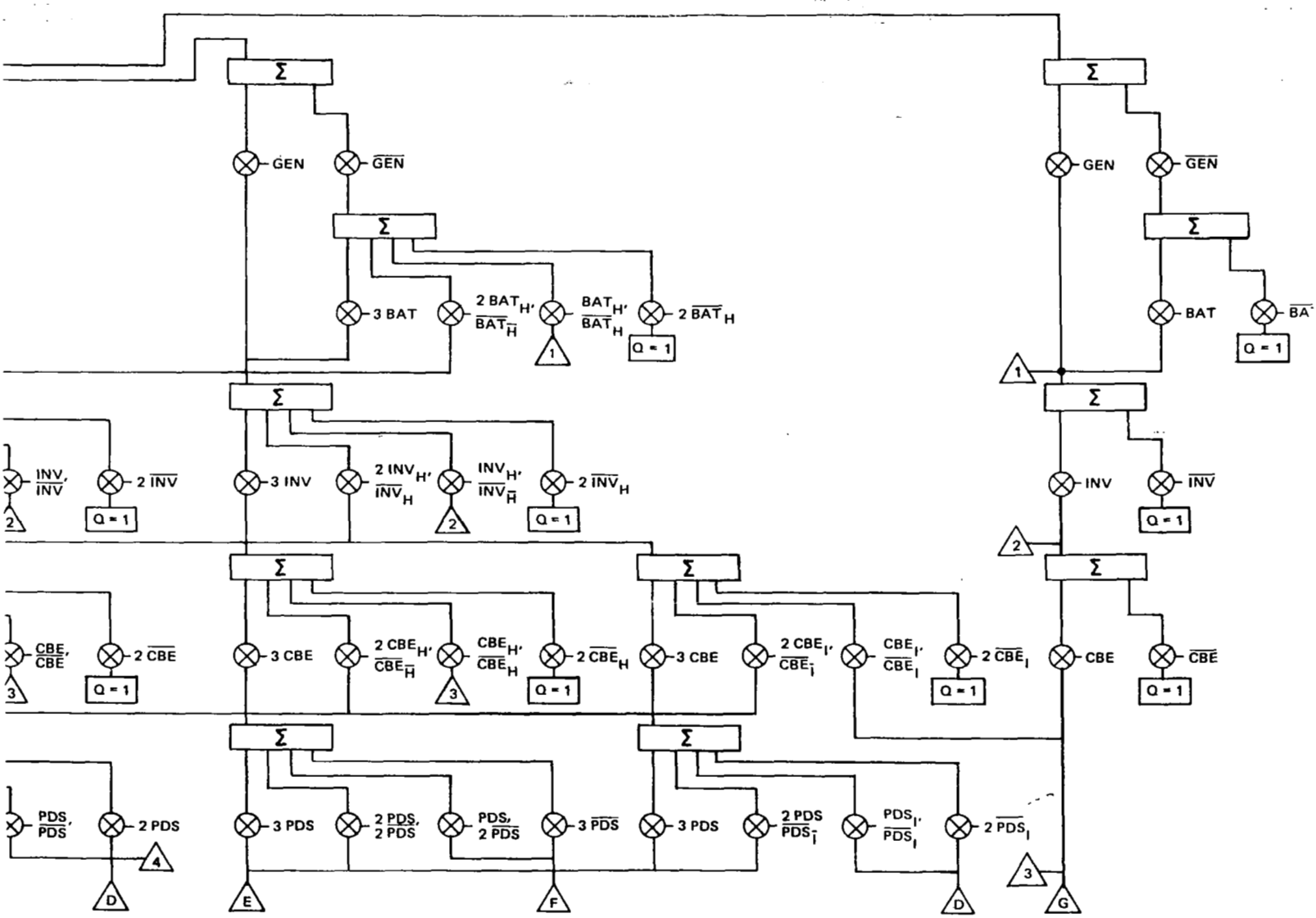


Figure 24. Diagram of F-8 DFBW unreliability equations modified to reduce major error sources.

		1	2	3	4	5	6	7	8	10	11	12	13	
HYDRAULICS	1	2.83E-10 2.12E-10	6.54E-11	6.11E-12										
GENERATOR	2	2.12E-10 2.11E-10	7.41E-13		0.00E+00									
BATTERIES	3		1.24E-09 2.11E-10	9.11E-10	7.38E-11	4.54E-11								
INVERTERS	4	2.11E-10 9.82E-11	1.12E-10	9.25E-13	9.54E-14					8.51E-07 8.36E-07	1.35E-08	2.09E-09		
COMMON BASE ELEC	5	9.82E-11 2.56E-13	9.74E-11	5.02E-13	6.07E-14					8.36E-07 8.26E-07	8.52E-09	1.54E-09		
PRIMARY DIGITAL SYS	6	2.56E-13 1.23E-14	5.64E-17	2.44E-13	1.24E-16					8.26E-07 1.67E-07	6.59E-07	5.02E-10		
PITCH BYPASS	7				3.52E-08 1.78E-14	1.95E-13	3.52E-08	1.27E-12					2.17E-04 3.03E-07	2.1
RT PITCH SW	8	1.24E-14			1.78E-14			6.01E-10		1.67E-07			3.03E-07	
RT PITCH ACT	9	1.23E-14			1.78E-14			2.72E-12		1.57E-07			2.93E-07	
LEFT PITCH SW	10		1.11E-07			1.11E-07			2.45E-05		4.09E-04			4.0
LEFT PITCH ACT	11		1.11E-07			1.11E-07			1.11E-07		3.85E-04			3.8
ROLL BYPASS	12				5.43E-15								1.36E-07	
RT ROLL SW	13	1.38E-21			1.92E-21			9.28E-17		6.84E-11			1.05E-10	
RT ROLL ACT	14	1.38E-21			1.91E-21			4.20E-19		6.43E-11			9.83E-11	
LEFT ROLL SW	15		1.24E-14			1.72E-14			3.79E-12		1.67E-07			2.5
LEFT ROLL ACT	16		1.23E-14			1.71E-14			1.71E-14		1.57E-07			2.4
YAW BYPASS	17						1.54E-07							
YAW SW	18			1.11E-07			1.11E-07		2.45E-05			4.09E-04		
YAW ACT	19			1.11E-07			1.11E-07		1.11E-07			3.85E-04		
		1	2	3	4	5	6	7	8	10	11	12	13	1

	14	15	16	17	18	19	20	21	22	23	24	25	26	27		
															1	HYDRAULICS
			1.74E-07 1.73E-07	2.62E-10								1.94E-04 1.93E-04	3.29E-07		2	GENERATOR
				4.39E-07 1.73E-07	9.11E-10	7.38E-11	4.54E-11						5.50E-04 1.93E-04	3.57E-04	3	BATTERIES
			1.74E-07 1.58E-07	3.73E-11	1.35E-08	2.09E-09						1.93E-04 1.48E-04	4.57E-05		4	INVERTERS
			1.58E-07 1.48E-07	3.25E-11	8.52E-09	1.54E-09	8.17E-07 8.07E-07	3.25E-11	8.52E-09	1.54E-09		1.48E-04 1.08E-04	3.93E-05		5	COMMON BASE ELEC
			1.48E-07 1.47E-07	6.73E-10	1.27E-12	6.44E-16	8.07E-07 1.47E-07	2.24E-10	6.59E-07	5.02E-10					6	PRIMARY DIGITAL SYS
E-04 E-07	2.17E-04	1.17E-08				1.83E-07 1.48E-07	5.43E-11	3.52E-08	1.27E-12			1.08E-04			7	PITCH BYPASS
E-07			1.48E-07			1.48E-07			1.67E-07			7.57E-08			8	RT PITCH SW
E-07			1.48E-07			1.48E-07			1.57E-07			7.32E-08			9	RT PITCH ACT
	4.09E-04			3.85E-04			3.85E-04			4.09E-04			2.05E-04		10	LEFT PITCH SW
	3.85E-04			3.85E-04			3.85E-04			3.85E-04			1.92E-04		11	LEFT PITCH AC
E-07						7.04E-11						3.39E-08			12	ROLL BYPASS
E-10			5.69E-11			5.69E-11			6.43E-11			1.31E-11			13	RT ROLL SW
E-11			5.69E-11			5.69E-11			6.05E-11			1.23E-11			14	RT ROLL ACT
	2.56E-07			1.48E-07			1.48E-07			1.57E-07			6.40E-08		15	LEFT ROLL SW
	2.40E-07			1.48E-07			1.48E-07			1.48E-07			6.01E-08		16	LEFT ROLL AC
		6.25E-04						3.85E-04						3.13E-04	17	YAW BYPASS
		4.09E-04			3.85E-04			3.85E-04		4.09E-04				2.04E-04	18	YAW SW
		3.85E-04			3.85E-04			3.85E-04		3.85E-04				1.92E-04	19	YAW ACT
3	14	15	16	17	18	19	20	21	22	23	24	25	26	27		

Figure 25. Results for F-8 DFBW unreliability with modified system.

Table 22. Failure data for the modified F-8 DFBW system.

t (h)	Probability of Failure ($\times 10^{-9}$)	Average Failure Rate ($\times 10^{-9}$/h)	Instantaneous Failure Rate ($\times 10^{-9}$/h)
0.5	0.4	0.07	0.25
1.0	0.28	0.28	0.95
1.5	0.96	0.64	2.03
2.0	2.27	1.14	3.60
3.0	7.68	2.56	8.00
5.0	35.72	7.14	22.00
10.0	288.88	28.88	88.20

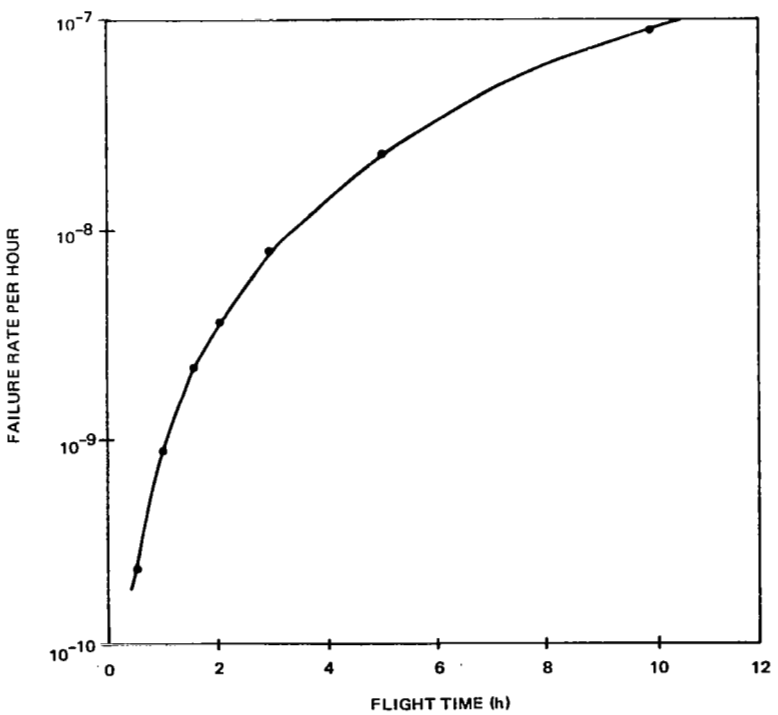


Figure 26. Instantaneous failure rate of the modified F-8 DFBW system as a function of time.

SECTION 7

REFINEMENT AND EXTENSION OF THE ANALYSIS

The reliability analysis forming the major part of this study has accounted only for random failures of component parts. Further, each failure has been assumed to be "hard", i.e., causing a complete loss of that element with no effect on any other element. Also, any failure to detect, identify, and properly respond to a fault has not been considered. In other words, coverage is assumed to be perfect. The analysis is also static. No distinction has been made for the sequence in which failures occurred.

This section covers refinements and extensions to the analysis that can improve its accuracy. First, possible refinements of the analysis of random-failure hazards are discussed, including the effects of failure modes, coverage, and failure sequence. Next, the extensions of the analysis to include other hazards in addition to random failures are discussed. Some of the factors considered are: interaction between degraded system performance and pilot performance, damage hazards, and software faults. In most cases, these refinements and extensions can be incorporated into the analytical structure described in Section 8.

The analysis in this section is, by nature, much less precise than the random-failure analysis described in the previous sections. The intention here is to identify as many other factors as possible that may influence the actual failure rate. The characteristics of these factors are discussed, and opinions are expressed on their potential significance. The primary purpose of these discussions is to keep the random-failure analysis in the proper perspective.

Effects of Failure Modes

The analysis performed so far has assumed that all failures are hard failures that would affect only one element. In most cases, this assumption is conservative. Often, failures in some of an element's components will not cause complete loss of the critical functions of that element because the failures have occurred in circuits that are not critical to the element's primary function. In other cases, a

failure may be charged to a component because its performance is not within specifications, even though the component is still able to perform its required function. Also, the sensitivity of the circuit to the complete failure of some components may be low enough that the required functions are still available.

Any refinement to account for these less-than-total failure modes will tend to reduce the predicted value of system unreliability. That probability is already very low compared to normal mission requirements and to the uncertainty due to other potential hazards. A refinement of the analysis in this direction was considered unnecessary, and the more conservative analysis was allowed to stand.

It was considered more important to be sure that there were no failure modes that would tend to increase the system unreliability, such as a failure mode of a component in one element that would prevent the use of another element. The circuit that is most likely to have this type failure mode is the BASE primary-system-to-bypass-system switch, where a failure in one switch could cause the failure of another switch. Thus, additional analysis was carried out on this circuit.

The critical components in both the right and left pitch switches are shown in Figure 27. The switch operates by simultaneously causing one transistor on each side to ground its input, and the other transistor to be open, allowing its corresponding input to pass. The critical question is whether there are any failures modes of any of the components that can cause a loss of both right and left channels. Failure modes of the transistors are assumed to be "fail open" or "fail short",

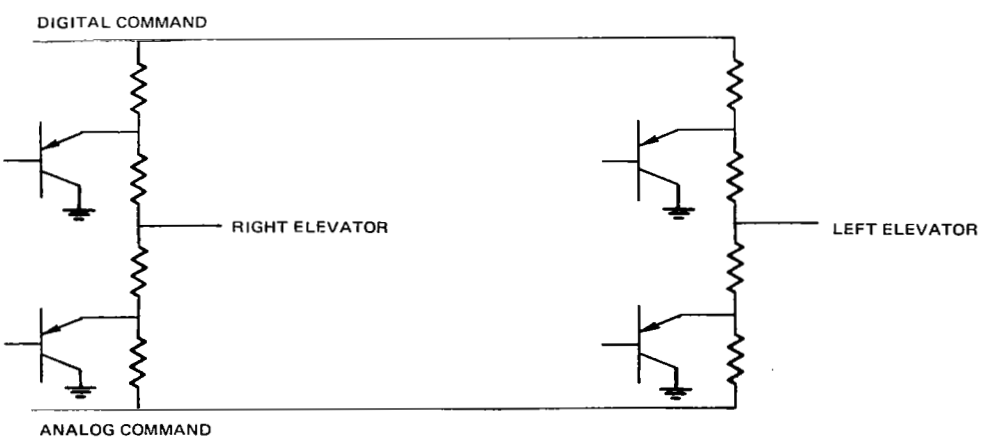


Figure 27. Critical components of two digital/bypass switches.

and the only failure mode of the resistors is assumed to be "fail open". A failure modes and effects analysis (FMEA) of this circuit showed that no single failure state would affect both channels.

A limited analysis of the rest of the system did not uncover any other failure mode that would increase the unreliability of the system. This is a reflection of the good design of the system and cannot be assumed in general.

The situation where a failure mode does cause loss of another element can be included within the analysis structure that was developed in Section 3. Situations such as this can be accounted for by expanding the number of events defined for the state of that element. For example, failed open and failed closed switch failures could be distinguished with the appropriate probabilities assigned to each condition. A distinction could then be made in computing the conditional unreliability of the rest of the system on the basis of the state of the system created by these different failure modes.

Effects of Coverage

Coverage is defined as the conditional probability that the system will continue to perform its required function given that a failure occurs. This implies that there are sufficient resources remaining to perform the required functions. Coverage is a very important parameter in a complete reliability analysis model. It accounts for the inability of the system to either detect, identify, or successfully respond to a failure. If a system must detect and identify a failure and then reconfigure itself to remove the failed element or incorporate a spare unit, and there is a chance that this process will fail, the coverage will be less than 1.

In a triplex system, the coverage of a second failure may be different from the coverage of a first failure. Coverage of a first failure in triplex voting systems is often assumed to be 1, but even if it is slightly less than 1, it can be a dominant factor (see Reference 14).

A review of the F-8 DFBW system revealed few situations where coverage as a separate term would significantly influence the estimate of unreliability. Most of the F-8 DFBW system is designed as a triply redundant system with all three channels permanently wired in and selected by midvalue-logic circuits. Thus, any failure of these

circuits to reject a failed signal has already been included in the failure modes of that element. In most cases, the F-8 system does not have separate circuits which can detect a failure and then take positive action to reconfigure the system on the basis of the detected failure. There are a few exceptions which will be discussed.

In most cases, the assumed coverage is thus implicit in the configuration of the basic equations. The coverage of the first failure is generally 1, and the coverage of many second failures is 0. In other words, when the second of the three channels fails, that entire stage is eliminated. For example, there is considerable self-test within each digital channel, and it is used to remove a digital channel from the operating set. However, this self-test is not used to select between two remaining channels and allow continued operation on the one good channel after a second failure; a second failure causes transfer to the bypass system.

No plausible scenario could be identified that would prevent an automatic transfer to the bypass system after the second digital system failure except for a unique set of simultaneous failures. If one digital channel failed and the failure were not detected by its own self-test, then the detection would be made by comparison with the output midvalue-select circuit. A complete system failure would result only if both remaining digital channels failed and both self-tests also failed. The probability of these simultaneous events is negligible compared with other sources of failure. In any case, if the failure to transfer occurred at a noncritical time, the pilot could perform the transfer manually.

There are at least two areas in the F-8 DFBW system where coverage could be a factor. It was assumed in the random-failure analysis that the system would continue to operate as a single-channel system after a second hydraulic system failure. This transfer does not occur automatically. The pilot must observe a single hydraulic system failure light, look at the pressure indicators to see which system has failed, and then switch the servo engage switches to manual mode in each axis for the one remaining good primary hydraulic system. The analysis optimistically assumed that the probability that this would occur was 1.

To obtain some measure of how important this coverage factor can be, two questions can be asked:

(1) How much less than 1 can the coverage become before it starts to be significant?

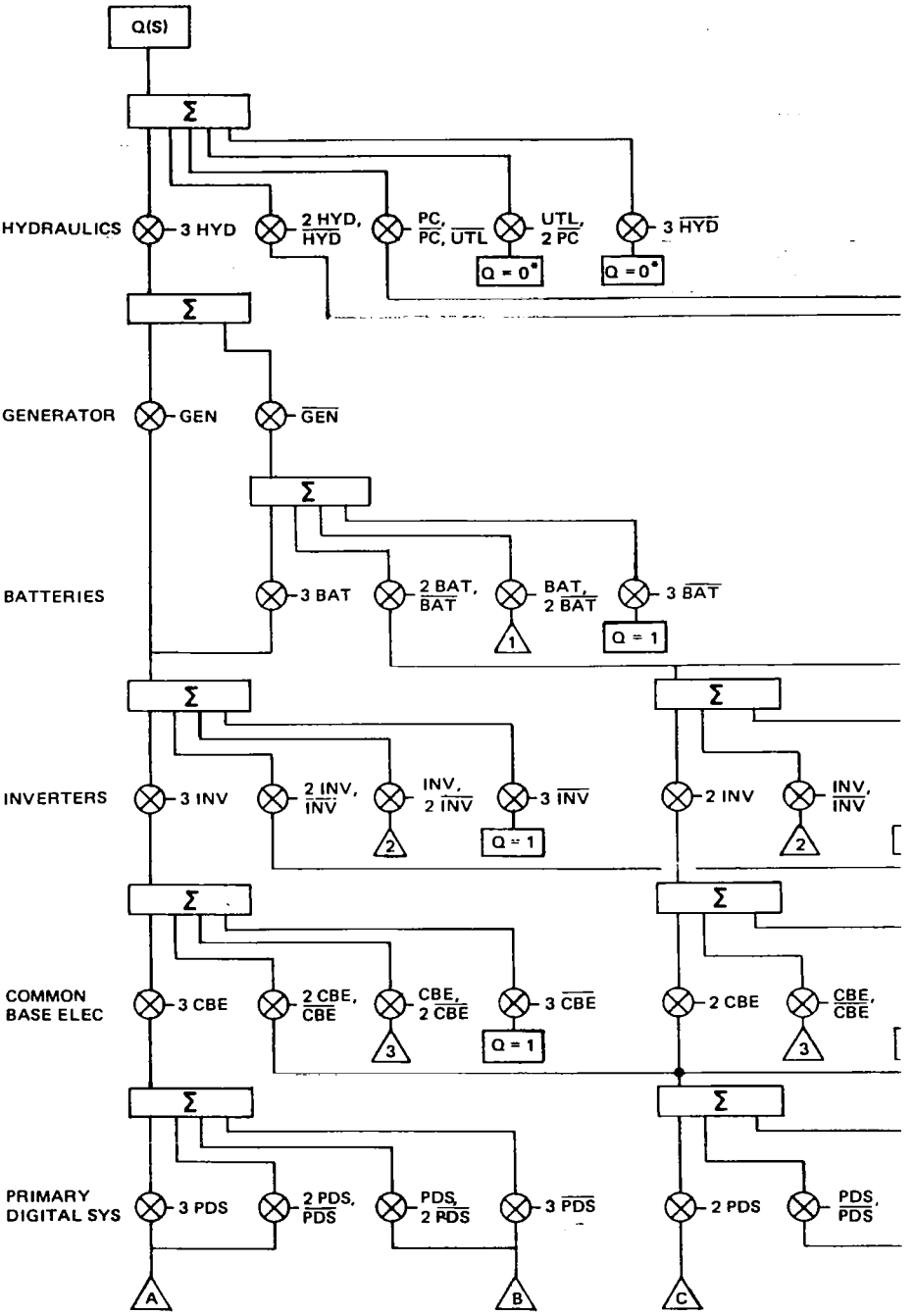
(2) Is this value of coverage plausible?

The value of the analysis structure that was constructed for answering these kinds of questions can be illustrated. The method that can be used to insert this coverage factor into the structure is shown in Figure 28. Values can be assumed for coverage, and the effect can be measured using the numbers from Figure 23. If coverage is 0, the unreliability of the system is increased by only 50 percent. If the coverage is assumed to be 90 percent, i.e., there is one chance in ten that the failure happens at a critical time or for some other reason the pilot fails to make the switch, the unreliability would only be increased by 5 percent, which is insignificant relative to the accuracy of the other numbers.

The actual coverage value that should be used for a human operator is difficult to obtain. If this number were important, the results of human factors research or simulations on the "iron bird" may be used to obtain a more accurate estimate of the number. For this study, one-in-ten seemed to be excessively large, and thus it is felt that this factor can safely be ignored. If the system modifications discussed at the end of Section 8 were made, the transfer to a single channel would be automatic and the human coverage factor would be removed.

One area was identified where a hardware failure could lead to coverage of less than 1. Each BASE channel has a power-supply monitor that is intended to detect any failure in the dc power supply (generator or battery), ac power supply (inverter), and its own internal power supply (common BASE electronics). These failure-monitoring discretes are cross-wired so that if these supplies fail in two channels, the remaining good channel would be automatically put into single-channel mode. If the monitor circuits failed in either of the two failed channels, the system would not go into single-channel mode and the two-out-of-three voters would cause the whole system to shut off.

The effect of coverage can be accounted for by inserting an additional level (as shown in Figure 29) in the paths defined by the transfer triangles 1, 2, and 3 in Figure 10a. The potential impact of this addition can be determined by tracing the numbers in Figure 30. The effect of this modification will be to add an additional term to the numbers circled in column 25 before they are transferred to columns 3 and 4. These factors will thus not be significant unless one minus



*LOSS OF AIRCRAFT DUE TO COMPLETE HYDRAULIC FAILURE NOT ALLOCATED TO ELECTRONIC FLIGHT-CONTROL SYSTEM.

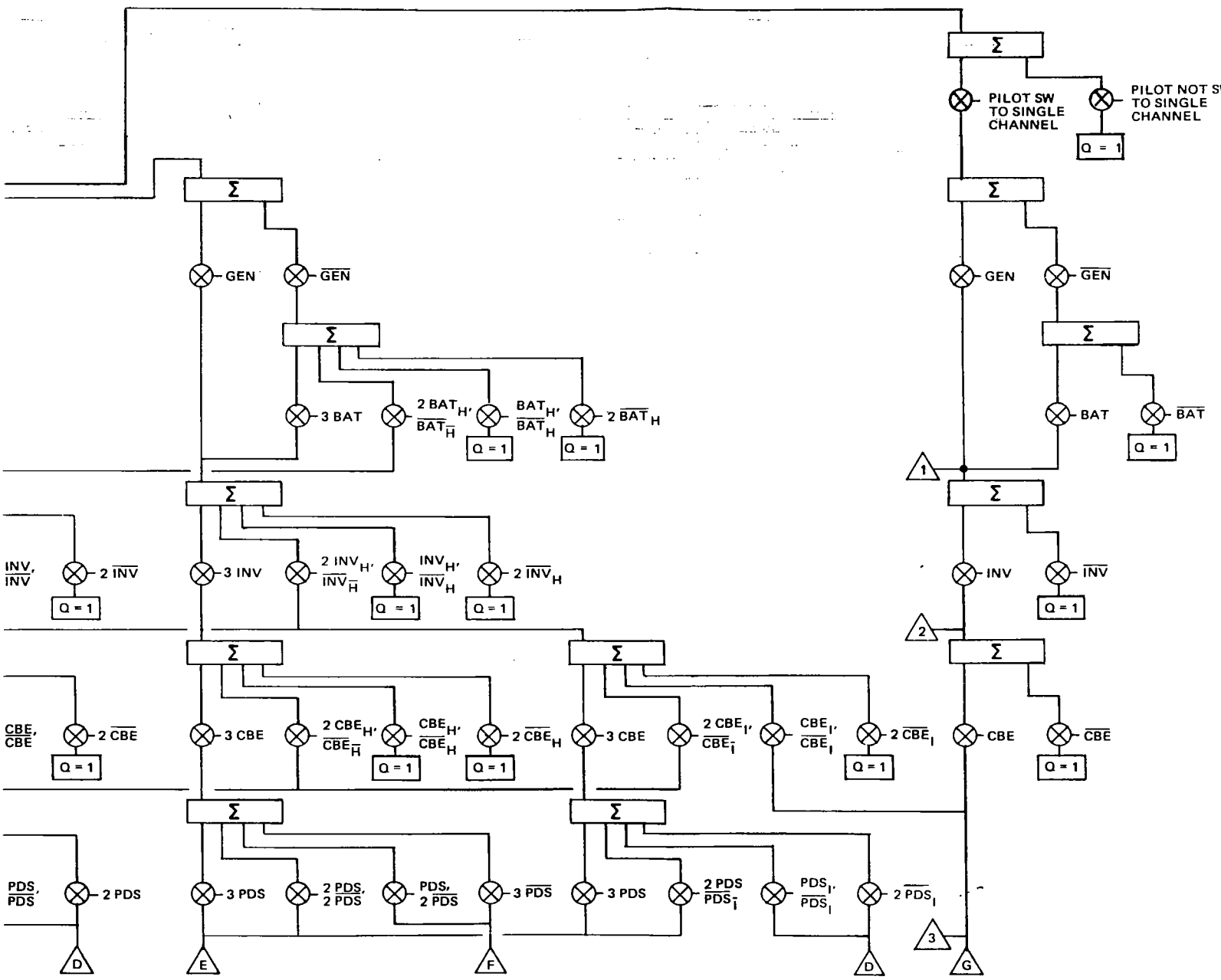


Figure 28. Diagram of F-8 DFBW unreliability equations, including pilot coverage of hydraulic failures.

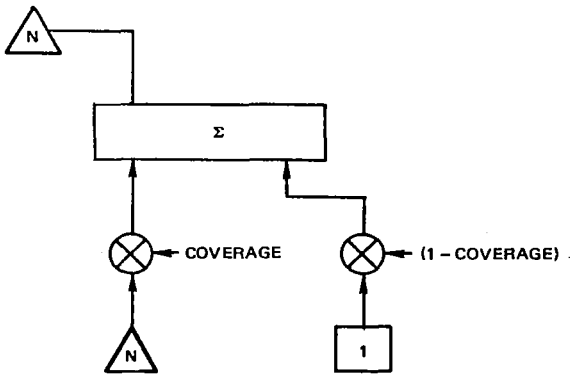


Figure 29. Additional level to insert effects of lack of coverage of power failures.

the coverage is large relative to numbers in the range of 1 to 2×10^{-4}. No analysis was performed on this monitor circuit, but it is relatively simple and would have a failure rate somewhere between the primary/bypass switch and the inverter (i.e., between 1 and 5×10^{-5}). If this assumption is true, the effect of a coverage failure will not be significant. The sensitivity of the analysis to an error in this assumption can be tested by tracing the effect of these error modes at higher levels. As can be seen by the numbers circled in columns 1 to 4 in Figure 30, the terms affected by coverage are being added to terms about two orders of magnitude larger. A failure in coverage will not make any ultimate contribution to the system unreliability unless the MTBFs of these circuits were around 100 hours, and they are at least two orders of magnitude better than that.

Effects of the Dynamics of the Failure Process

The failure-analysis technique used in this study assumes a static system. The equations give the probability that the system will have failed by the end of the specified time period, and do not consider when the failures occur or recognize the order in which they occur. A characteristic of the design of the F-8 DFBW system is that, in almost all cases, the dynamics or order of failures is not significant.

In most cases, the configuration of the F-8 system is not changed on the basis of failures. Where there is reconfiguration, no particular added vulnerability is found to exist during the reconfiguration time. The ultimate result of a second failure is the same whether it occurs during the reconfiguration time or at any other time.

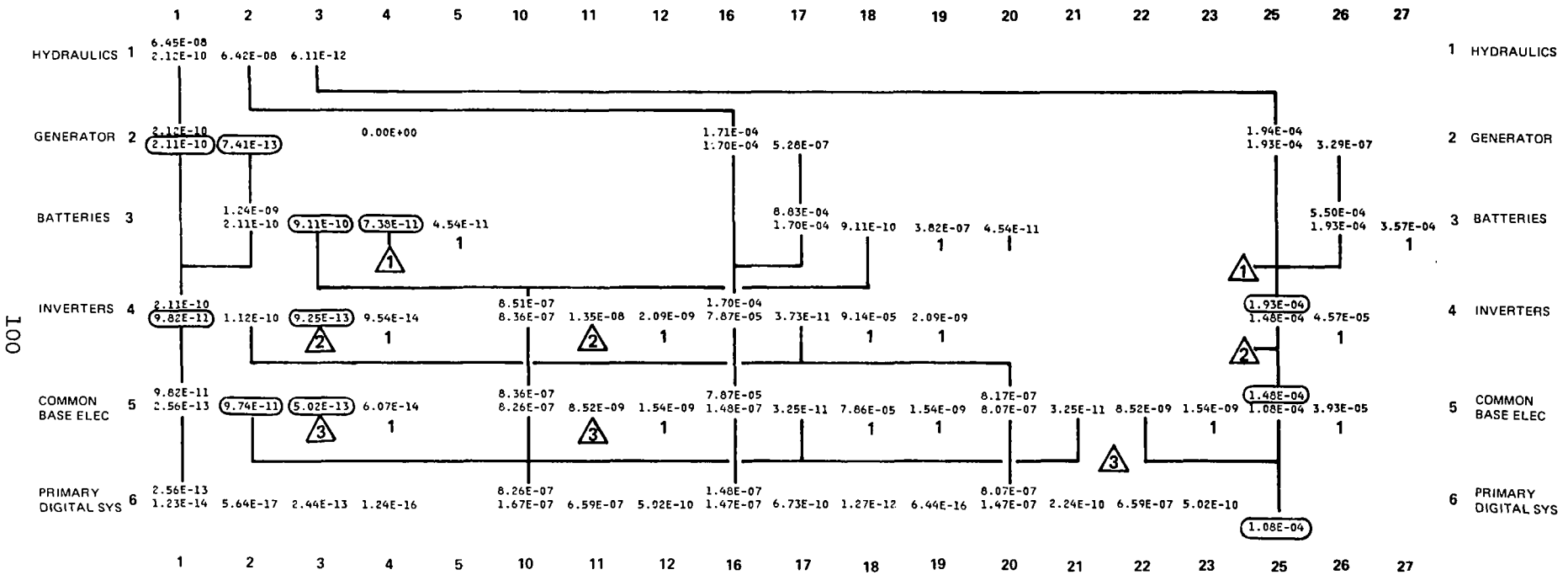


Figure 30. Numbers important to coverage of power failure.

The order in which elements fail was also found not to be significant in most cases. One set of situations was found, however, where the sequence would have an effect. These were the situations where there were two failures in either the batteries (with a generator failure), the inverters, or the common BASE electronics, and also a hydraulic system failure. If both the failures in the power supplies occurred before the hydraulic system failure, the system would automatically be switched to single channel and would continue to operate as long as the hydraulic failure was not in that channel. If the hydraulic failure occurred before the second power-supply failure, the transfer to single channel would not be automatic and the system would fail.

The effect of the failure sequence can be incorporated into the analysis structure by expanding the events that define the state of the failures at that level, including sequence. This expansion of events can be illustrated by the equation for inverters in the case where there is a hydraulic failure (refer to Figure 10a; the inverter row at column 8). This equation originally had four events defined:

(1) Three inverters good.

(2) Two inverters good with good hydraulics and the inverter with failed hydraulics failed.

(3) One inverter good with good hydraulics, one inverter failed with good hydraulics, and the inverter with failed hydraulics good or failed.

(4) Two inverters failed with good hydraulics, the inverter with failed hydraulics good or failed.

Events 1, 2, and 4 would stay the same, but event 3 would be divided into three events as follows:

(3a) One inverter good with good hydraulics, one inverter failed with good hydraulics, and the inverter with failed hydraulics good.

(3b) One inverter good with good hydraulics, one inverter failed with good hydraulics, and the inverter with failed hydraulics failed, with one of two inverter failures occurring after the hydraulic failure.

(3c) One inverter good with good hydraulics, one inverter failed with good hydraulics, and the inverter with failed hydraulics failed, with both inverter failures occurring before the hydraulics failure.

The appropriate probabilities can be computed for these events, and then they would be multiplied by the appropriate conditional unreliabilities for the rest of the system in that particular state.

The error caused by not considering this term in the F-8 DFBW system is negligible. The first event (3a) dominates the other two because it is proportional to Q of the inverter, while the other two are proportional to Q^2 and thus will be at least four orders of magnitude smaller.

If the order of failures had been important, the total impact on the equations would have been considerably more involved than the one equation illustrated. Similar equations would be necessary for the batteries and common BASE electronics, and several additional equations for combinations of failures involving battery, inverter, and common BASE electronic failures. For the analysis of a system where failure sequence was important, a reassessment of the advantages of a Markov analysis may be advisable.

Interaction of System Failure with Pilot Performance

The analysis performed here does not take into account the possible effects degraded system performance might have on pilot performance. The assumption made for this study is that if the flight-control system is capable of controlling the aircraft, the probability is zero that the aircraft will be lost. For example, it was assumed that the aircraft can be safely landed with only one elevator or with only the rudder to maintain roll.

It is obvious that the potential for an incident in performing a critical maneuver, such as landing, with a nonstandard control response is much greater. For example, if a quick-response pitch command is needed, the unwanted roll resulting from using the elevator on only one side could be hazardous. This increased hazard should be charged to the flight-control system.

This factor can be included within the model by inserting the appropriate numbers for the final conditional unreliabilities at the end of the equations. For example, at the bottom of Figures 10b, c, d, and e, the number is now 0 for the unreliability at the system, given that any minimum combination of control surfaces is available. These numbers could be made somewhat higher than zero to reflect the probability of a flight-control-induced accident.

A numerical value for these probabilities will not be easy to obtain. It is likely to be subjective and to depend on many factors, such as pilot experience and competence. This number could be estimated by a survey of pilot opinions that would provide a description of the expected characteristics of the aircraft, and would ask how many times the aircraft would survive if it were landed in this condition unexpectedly by 100 pilots. This number could be estimated more accurately by setting up these conditions in a simulator and injecting them unannounced with other disturbances to measure pilot performance. A high degree of confidence many not be attached to these numbers, but to include them may be more realistic than to ignore the factor completely.

Contribution of Damage to Failure Rate

Physical damage to the electronic flight-control system can be a significant factor in the failure rate. A preliminary study was made that estimated the failure rate due to damage of an electronic system in a commercial aircraft to be in the range of 10^{-8} to 10^{-9} per hour. These estimates would not be directly applicable to the F-8, but do indicate that damage could be an important consideration.

No attempt was made to obtain a quantitative estimate in this study of physical damage probabilities. This estimate would depend on a detailed study of how the system is installed in the aircraft, a cataloging of all possible events that could cause damage to the electronic flight controls, an estimate of the probability of each of those events, and finally an estimate of the effect the event would have on the electronic flight control.

A preliminary look at the F-8 DFBW system indicated that the elements most vulnerable to damage were the BASE electronics unit and various points along the cables running from the BASE electronics to the actuators, particularly those in the tail. The BASE units are stacked one atop the other in the left gun bay as shown in Figure B.10. Any event that could damage one box would have a relatively high probability of damaging all three. Since all actuators are commanded from these boxes, if all were sufficiently damaged, the aircraft would be lost. Some possible events that could damage these units are an uncontained failure in one of the units (e.g., a power-supply failure and the simultaneous failure of the circuit breaker resulting in a fire), a battery explosion, a hydraulic leak, and the loss of the common access panel with associated wind or

rain damage. One of the damage events in the study of damage to commercial aircraft was due to hydraulic mist fire. Hydraulic fluid is not flammable at reasonable temperatures, but in one incident it was found that the mist created by a very small hole was flammable at room temperature and the resulting fire destroyed all cables in one compartment of the aircraft.

A quantitative estimate for the F-8 would require gathering of damage data from a fleet of F-8 or similar type aircraft flown in similar ways, and then an analysis of how these events might have damaged the flight-control system. This effort is beyond the scope of the present study.

It was assumed, based on the preliminary study of commercial damage events, that damage would not be a significant contributor to the system with a failure rate of 6×10^{-8} per hour or greater. However, if the system were improved by an order of magnitude or more, damage would have to be studied seriously.

Software Errors

The possibility of a generic fault that would be present in all versions of a redundant system has been one of the chief concerns of digital flight-control system designers. The fear of this type of failure and the difficulty of proving that it does not exist to an acceptably low level is one of the primary reasons for the existence of a dissimilar backup system on the F-8 and other fly-by-wire systems.

Software errors are in a different and much more difficult to handle category than the random failures discussed in Section 2. Various techniques have been proposed to try to estimate software reliability.[15,16] One technique is to attempt to estimate the rate at which new faults will appear based on the declining rate at which they appeared in the past. Another method is to purposely embed errors and see how thoroughly the system testing removes these errors. To date, none of these techniques have been developed to the extent that they can provide a reasonable degree of confidence that the high-reliability requirements have been met. So far, the most promising approach seems to be the use of very disciplined structured methods of writing the software in the first place. These techniques avoid the introduction of errors which become so difficult to detect later.

The software for the F-8 DFBW was very carefully written, controlled, and tested (see Section 5 of Reference 17). No attempt was made in this analysis to apply any of the existing techniques to develop a quantitative estimate of the probability of a software failure. The following paragraphs discuss how many of the effects of software faults could be inserted into the model and what the extent of these effects could be for this particular system.

The sensitivity of the unreliability of the total system to software faults is considerably reduced by the existence of the bypass system. Software faults can thus be divided into three categories. The faults that are expected to be most likely will have a passive effect on the total system. Many of the errors that are possible would cause the computer to get trapped in a loop, stop executing, or violate one of the many hardware and software fault-detector devices. This failure would cause automatic transfer to the bypass system. If a probability could be estimated for this type of error, it could easily be included within the model by adding it to the probability that three primary digital systems fail due to random failures. From Figure 10 it can be seen that three failed computers are equivalent to two failed computers. Thus, this category of software failure will have no influence on the equation unless its probability is in the range of 10^{-6} to 10^{-5} per hour, which is the probability that two digital channels will fail. The probability of this type of software failure would have to be as large as 10^{-1} per hour to influence the final total system unreliability in the most significant digit. The amount of time accumulated on the system with no failures of this type provides a high degree of confidence that the probability of this failure is several orders of magnitude smaller than 10^{-1} per hour. Thus, it can be concluded that this category of software failure will make no measurable contribution.

The second category of possible software failures which would be much less probable are those that are still passive but allow the program to continue to operate at least well enough to avoid detection by the detection devices. This error would not be detected by the output comparison voters, since all three computers would agree. There would thus be no automatic transfer to the bypass system. This type of failure would be obvious to the pilot because control inputs would have no effect. The immediate reaction of the pilot would be to manually transfer to the bypass system.

The contribution of this type of failure will thus be the same as that of the first category with two additional factors. One factor is the probability that the pilot will not recognize the failure and/or will not take proper action. The other additional factor is that the failure may happen at a very critical moment such that manual transfer could not be made in time. The amount of time that would be critical is expected to be only a few seconds per flight. Also, the probability that a pilot would not react properly is expected to be much less than 10^{-3} per hour. The probability that this type of software fault could occur would have to be around 10^{-5} per hour to be significant.

The third category of software failure which is expected to be even less probable is an active failure. This failure would cause all computers to simultaneously issue a large command to at least one of the surfaces. The risk of this type of failure is very similar to the previous one. The pilot would certainly be aware of the failure and would manually switch to the bypass system in most cases. However, the aircraft can very quickly be put into a vulnerable position, and the critical time will thus be greater. The critical time during a typical flight where recovery would be unlikely is assumed here to be tens of seconds approaching a minute, i.e., an order of magnitude greater than the previous category. The probability of this type failure is assumed, however, to be at least an order of magnitude smaller.

Although the probability that a software failure will occur was not estimated directly in this analysis, the ways in which software faults could contribute to system unreliability were identified along with the levels of software failure rates that would produce a significant effect. Experience with software errors during the test program gives confidence that the failure rate will be well below those levels for this system.

SECTION 8

CONCLUSIONS, OBSERVATIONS, AND RECOMMENDATIONS

The primary conclusion drawn from this study is that the F-8 DFBW system has a very high predicted reliability. A conservative estimate of the probability of loss of the aircraft due to random failures is 6.45×10^{-8} for a 1-hour flight. No nonrandom hazard such as damage or software error could be identified that would significantly increase that probability. The probability of loss of the primary digital control mode for a 1-hour flight is predicted to be 7.82×10^{-6}.

The greatest contributor to the failure probability was found to be the hybrid situation with a hydraulic power failure in one channel and some electrical power failure in another channel. With a minor system modification, the power-monitoring logic could be modified to cause an automatic transfer to single-channel operation with any combination of electrical or hydraulic power failures. In this case, the probability of loss of aircraft from random failures can be reduced to 2.82×10^{-10} in a 1-hour flight.

Although the probability of loss of aircraft for a 1-hour flight is very low, the increase in the failure rate as a function of time is rapid. The failure rate in the basic system at 10 hours is 1.4×10^{-6}, an increase by more than an order of magnitude. The modified system failure rate at 10 hours is 8.8×10^{-8}, an increase by more than two orders of magnitude. Changes in the basic design would thus be necessary for commercial application either by increasing the basic reliability by adding additional redundancy or by adding active reconfigurations to replace failed units and thus keep the failure rate much closer to constant.

As an observation on the analysis process itself, the actual attempt to compute the numerical reliability gave a different perspective on the system than the one gained by showing that the system is fail-operational following any single failure. There is a real danger in

getting enmeshed in numerical reliability analysis. For this reason, many flight-control systems, including the F-8, are required to be fail-operational, fail-operational/fail-safe, dual fail-operational, etc. Much of the analysis that has been done on the F-8 DFBW system has shown that no single failure could cause a system failure. However, an attempt to compute the actual probability of system failure from all component failures and combinations of failures can give a more balanced perspective on the system failure process. This analysis has to include much practical judgment, and caution must be exercised to keep from overrating the validity of the results. With these reservations, it is believed that numerical analysis can direct efforts to the failure situations that are actually the most important, and avoid overemphasis on obscure failures which do not make any significant contribution to the total system failure rate.

It was not the intent of this study to develop any new analysis tools. However, the unreliability equation diagram turned out to be a very powerful and flexible technique in this analysis. It is not known if this technique or a similar one has been used before. If not, it is recommended that the technique be further investigated to see if it can be of more general application. If so, the technique could be further developed so that it could be more generally applied and be more widely publicized.

The Charles Stark Draper Laboratory, Inc.
555 Technology Square
Cambridge, Massachusetts 02139
November 1979

APPENDIX A

NASA ADVANCED FLIGHT-CONTROL PROGRAM*

The F-8 DFBW program has been carried out in two major phases. The first phase, which began in 1971 and concluded in 1973, successfully demonstrated the feasibility of using DFBW systems for the primary control of aircraft. This was accomplished by flight testing a single-channel DFBW system in the F-8 test aircraft. A surplus Apollo guidance and navigation system hardware was used for the primary flight-control system, and the basic F-8 mechanical system was completely removed. Forty-two flights were accomplished during this phase by six evaluation pilots, and a total flight time of 58 hours was accumulated. Historically, this was the first recorded flight of an aircraft using a DFBW system as its primary means of flight control with no means of mechanical backup.

The second phase of the program covered the period 1973-1980. The overall Phase II program objective was to establish a data base that can be used to design and develop practical DFBW systems for future aircraft. To accomplish this objective, the simplex Phase I system was replaced with a triplex multichannel DFBW system that uses fully programmable state-of-the-art digital processors for primary flight control. The first flight with the Phase II system occurred in August 1976. By the end of 1979, 73 flights were successfully accomplished. The flight-test program has been successful both in demonstrating a practical DFBW design concept that works and in developing required operational procedures. This is also the only airplane primary flight-control DFBW system currently in operation that does not employ a means for mechanical reversion in the event of failure.

The F-8 DFBW program is managed out of the Electronics Division of the Office of Aeronautics and Space Technology (OAST) at NASA Headquarters. The project office resides at the Dryden Flight Research Center (DFRC), which has functioned as the lead center during the entire program. Other

---

* This Appendix is an updated version of Section 3 of Reference 17.

NASA centers have been jointly involved. The Langley Research Center (LARC) has been responsible for development of certain advanced control-law concepts for flight-test evaluation of the Phase II system. The Johnson Space Center (JSC) has been jointly responsible for coordinating all shuttle-related flight tests.

A summary of the flight-test program accomplishments through 1979 is presented in Figure A.1. During the 73 flights accomplished thus far, all control modes have been engaged and evaluated using the various control tasks that are listed. The various data generated during the accomplishment of these flights has contributed greatly in expanding the technology data base for the DFBW controls, and in accomplishing the F-8 DFBW program objectives. Of primary significance is the fact that at no time during ground or flight tests of the flight-qualified system has a total digital flight-control system (DFCS) failure occurred requiring use of the analog bypass system.

- NUMBER OF FLIGHTS 73
- TOTAL FLIGHT TIME . . . . . 100 h
- MAXIMUM SPEED . . . . . MACH 1.2
- MAXIMUM ALTITUDE . . . . . 12,200 m
- MAXIMUM ACCELERATION 6g
- NUMBER OF PILOTS 4
- CONTROL MODES EVALUATED
  - DIRECT
  - STABILITY AUGMENTATION (SAS)
  - COMMAND AUGMENTATION (CAS)
  - AUTOPILOT:
    - MACH HOLD
    - ALTITUDE HOLD
    - HEADING HOLD
    - ATTITUDE HOLD
  - RIDE SMOOTHING
  - MANUEVER DRAG REDUCTION (MDR)
  - REMOTE AUGMENTATION (RAV)
  - SIDE-STICK CONTROLLER
  - ANGLE-OF-ATTACK LIMITER
- EVALUATION TASKS
  - ROUTINE FLIGHT
  - HANDLING QUALITIES INPUTS
  - FORMATION
  - TRACKING
  - MODERATE/SEVERE TURBULENCE
  - SIMULATED SHUTTLE LANDINGS
- FLIGHT-TEST VERIFICATION OF SHUTTLE RM SOFTWARE
- LOW-SAMPLE-RATE EVALUATIONS
- EVALUATION OF ANALYTIC REDUNDANCY MANAGEMENT
- EVALUATION OF PILOT WORKLOAD DURING SHUTTLE LANDING MANEUVER
- ESTABLISHED HARDWARE AND SOFTWARE OPERATIONAL PROCEDURES FOR DFBW SYSTEMS
- FIVE IN-FLIGHT COMPUTER FAILURES – DEMONSTRATED VALIDITY OF FAILURE DETECTION AND RECOVERY ALGORITHMS
- NO TOTAL SYSTEM FAILURE REQUIRING USE OF ANALOG BYPASS SYSTEM

Figure A.1. Flight-test summary.

APPENDIX B

SYSTEM REQUIREMENTS AND DESCRIPTION*

This appendix first describes the system requirements, both those specific to this program and those more generic specifications that would be typical of an advanced primary flight-control system. Next, the requirements that must be met to qualify the system for flight are given. Finally, the system is described. This description includes a brief overview of each of the units in the system, and explains how they are installed in the aircraft and how they are integrated into an operating system. Particular emphasis is placed on how fault tolerance is achieved to provide a very high level of functional reliability.

System Requirements

Mission-Specific Specifications

The requirements for the F-8 DFBW system can be divided into two categories: mission-specific and generic. The mission-specific requirements (shown in Figure B.1) are those determined by operational considerations, installation constraints, program funding, and schedule guidelines. The system was specified to be triplex, using government-furnished general-purpose digital computers, because a triplex configuration would present all the problems of multicomputer operation and could be installed within the space available in the F-8.

Program funding did not permit the procurement of an inertial platform set, as might have been desirable in this program. Therefore, aircraft-quality rate gyros and accelerometers were specified. The sensor and command lines were specified to be dedicated hardwire. Multiplexing was not possible within program funding.

Experience in the Phase I program and a state-of-the-art assessment in actuator stabilization resulted in the specification that this stabilization be done using analog components, outside of the digital computer,

---

* This appendix is a condensed version of Section 4 of Reference 17.

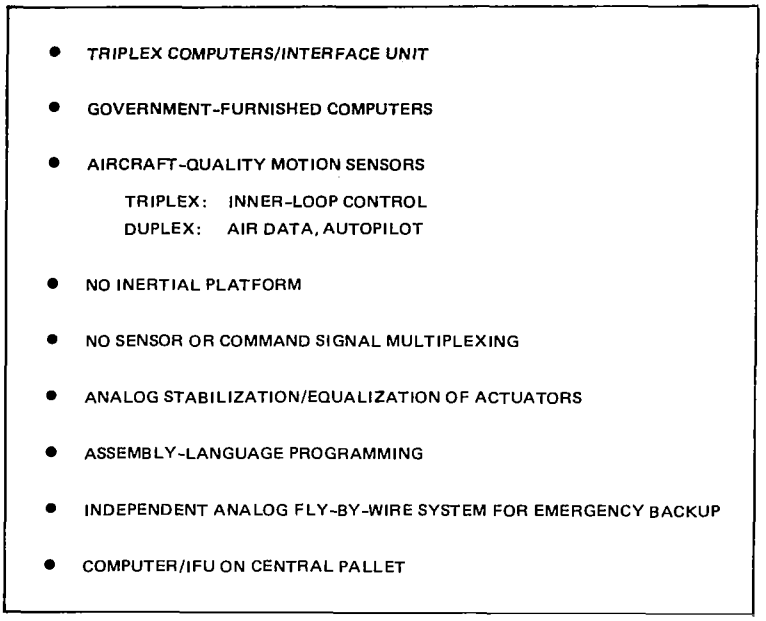


Figure B.1. Mission-specific requirements.

due to the sample rate requirements and computational burden. The use of a secondary actuator to drive the existing F-8 power actuators instead of a new integrated actuator was dictated by the burden of requalifying the primary actuation system of the F-8, including flutter clearance.

Assembly-language programming was specified for the F-8 DFBW system. This was due to the fact that a qualified high-order language was not avaliable for the flight computer at the time programming was initiated.

The research nature of the primary DFBW flight-control system required an independent dissimilar backup control system. The primary motivation was to protect against a common-mode software error that would disable the entire primary system.

Finally, the available space in the F-8 required custom packaging. The computers and interface units were specified to be mounted in a removable pallet assembly. Flight-control sensors were to be installed in easily accessible locations.

Generic Specifications

The generic specifications are those that tend to be independent of the particular application. They represent the fundamental operating characteristics of the system. In the case of the F-8 DFBW system, these requirements were selected to both tax the technology and to represent realistic and achievable specifications for a primary flight-control system.

Overall fault tolerance. - The key system fault-tolerance requirements can be stated in the following manner:

(1) No single fault in the primary digital system shall cause degraded inner-loop performance.

(2) No second fault in the primary system shall result in a hazardous situation.

(3) No sequence of sensor or display failures shall result in an automatic transfer to the bypass system.

(4) No single fault in the primary digital system shall result in a transfer to the bypass system.

(5) The loss of two computing channels in the primary system shall result in an automatic transfer to the bypass system.

(6) No primary system fault sequence shall prevent manual transfer to the bypass system.

Figure B.2 shows the fault-tolerance requirements for each major system. Generally, fail-operational requirements were specified for each system. A second like fault in any system has differing consequences, depending on the actual device faulted.

Primary-digital-system generic requirements. - The requirements for the primary digital system are of particular interest. Figure B.3 lists the major requirements that were imposed on the primary system. The overall fault-tolerance requirement, as explained previously, was fail-operational, with the failure of a second like major channel resulting in automatic transfer to the bypass system.

Single-channel digital operation was not permitted in the F-8 DFBW aircraft because of the experimental nature of the system. Automatic

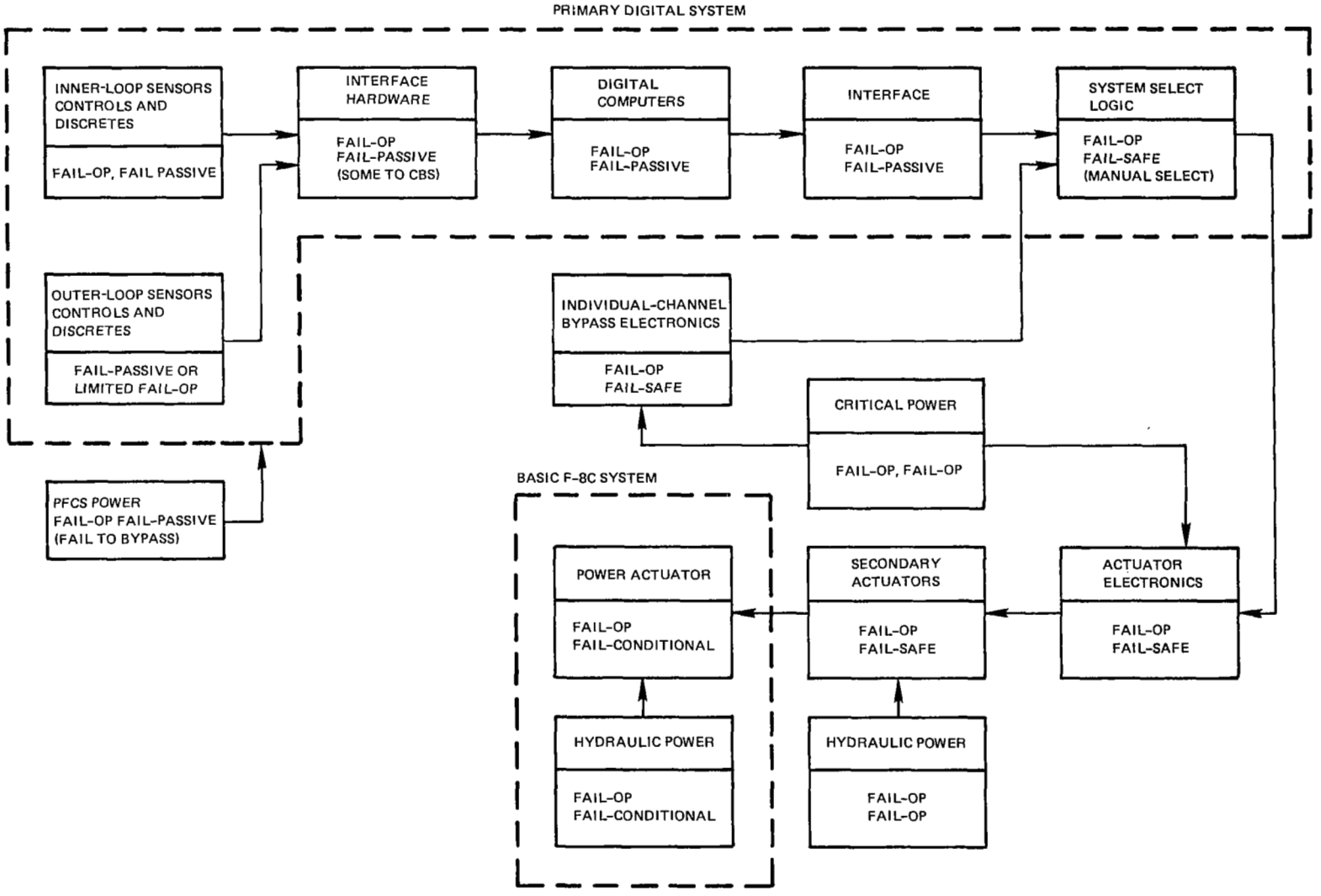


Figure B.2. Overall system fault-tolerance requirements.

AREA	REQUIREMENT	IMPLICATIONS
FAULT TOLERANCE	• FAIL-OP/FAIL-SAFE • SECOND FAIL TO BACKUP	• NO SINGLE-CHANNEL OPERATION • REDUNDANT POWER SOURCES
TURN-ON/OFF	AUTOMATIC INITIALIZATION FROM ARBITRARY TURN-ON/OFF SEQUENCE	NO CREW ACTION PERMITTED FOR START-UP
FAULT DETECTION	• HARD FAILURES TO BE DETECTED WITHIN 200 ms • HARD FAILURE DECLARATIONS TO BE IRREVERSIBLE	NO PROVISION FOR REINITIALIZATION BY PILOT
RECONFIGURATION	AUTOMATIC	NO CREW ACTION ASSISTANCE PERMITTED IN FAULT ISOLATION
TRANSIENT FAULT RECOVERY	FULLY RESTARTABLE IN ANY CONFIGURATION/MODE	CONTINUED OPERATION FOLLOWING: • TEMPORARY POWER LOSS • TRANSIENT HARDWARE/SOFTWARE PROBLEM
IMMUNITY TO FALSE ALARMS	DESIGN TO BE HEAVILY WEIGHTED TO AVOID FALSE ALARMS	NO QUANTITATIVE REQUIREMENT
OUTPUT COMMAND VOTING	ANALOG VOTING OF SURFACE COMMANDS	NO SOFTWARE VOTE OF SURFACE COMMAND
COMPUTER INTERCOMMUNICATION	MINUMUM POSSIBLE	REDUCE COMMON-MODE ERROR SOURCES
SYNCHRONIZATION	FRAME OR MINOR CYCLE ONLY	
CONTROL-LAW INTERFACE	MULTICOMPUTER STRUCTURE TO BE TRANSPARENT TO CONTROL LAWS	CONTROL LAWS WRITTEN AS FOR SINGLE COMPUTER
SYSTEM INTEGRITY	• FULL TIME • FULL CONTROL SURFACE AUTHORITY • FLIGHT CRITICAL CONTROL • NO MECHANICAL REVERSION	MAN-RATING REQUIRED PRIOR TO FIRST FLIGHT

Figure B.3. Generic system design requirements.

initialization from any arbitrary turn on/off sequence was specified so as to exclude the crew from any special action.

The 200-millisecond hard-failure fault-detection time was based on F-8 dynamic response at high dynamic pressure flight conditions. Hard failures were to be irreversible, with no provision for pilot reselection. All reconfiguration logic was to be automatic with no pilot participation permitted in the fault-isolation process.

The system was to be fully restartable in any mode following a transient fault. This meant that a channel or channels would be restored to normal operation following unspecified transient faults. There is always a problem in defining a transient fault. In the F-8 digital system, transient faults were divided into two categories: power loss (or apparent power loss) and all others.

The transient survivability times were defined as:

(1) Single-channel external-source power loss—no time limit.

(2) Multichannel power loss—40 milliseconds.

(3) Detected fault, any type—200 milliseconds.

This meant that a single channel was required to be restored to normal operation after being powered down for any indefinite period of time. This requirement is also necessary in order to be able to turn the system on. If power was lost by two or three channels for less than 40 milliseconds, the primary system was to be restored to normal operation and continue to be in control of the aircraft. If this power loss occurred for more than 40 milliseconds, the bypass system was to effect an automatic takeover. It should be noted that the primary system was still required to be restored to normal operation following a long power interruption, even though command had been handed over to the bypass system.

For detected faults, that is, for conditions where execution is apparently continuing, but where an abnormal condition has been detected, including an internal power supply fault, the transient time was specified to be 200 milliseconds. This is based on 10 attempts to restore normal operation at the nominal 20-millisecond minor cycle, and is the maximum time a fault can be tolerated at critical F-8 flight conditions. These requirements are illustrated in Figure B.4.

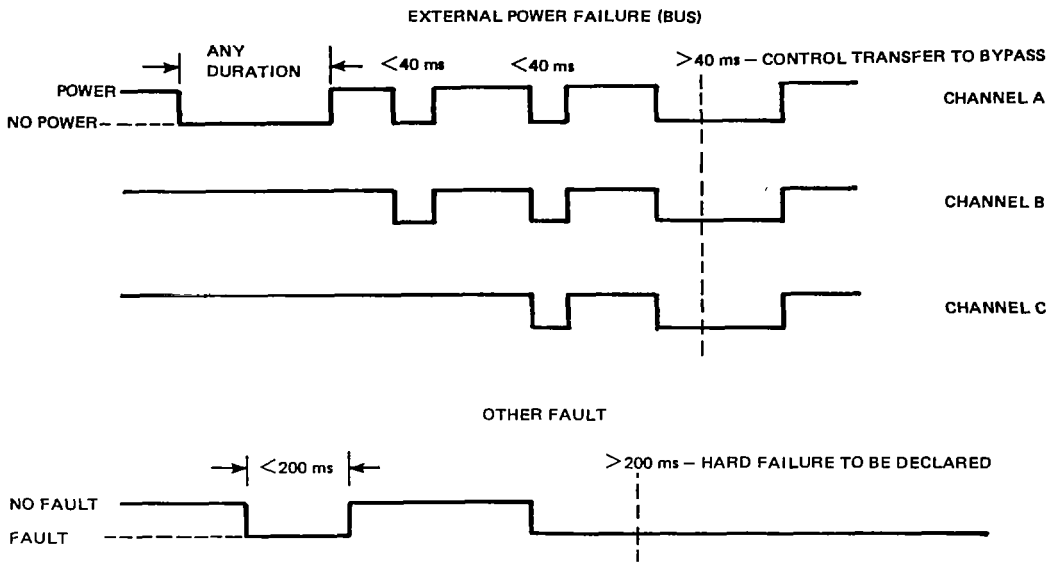


Figure B.4. Transient fault survivability requirements.

False-alarm immunity was recognized to be a critical characteristic of the DFBW system. A requirement was imposed that the system was to be weighted in favor of continued or restored operation in all possible cases. It was not known how this requirement could be proven analytically, thus no quantitative specification was given. Actual operating experience would give an insight into this feature of the system.

In the preliminary design it became apparent that special consideration had to be given to the problem of undetected digital system failures occurring in a sequence that would cause hazardous commands to be generated. The solution chosen was to require analog output voting on the digital-system surface commands. This approach was taken to protect against a catastrophic fault sequence in a manner independent of digital system software or failure-detection logic.

In an attempt to reduce the possibility of interchannel fault propagation, it was specified that intercomputer communication was to be kept to an absolute minimum, with design approaches deliberately avoiding complex computer intercommunications.

Synchronization was specified explicitly to be frame or minor cycle only. Thus the computers, while being tightly synchronized, would not be in exact step. This was specified in order to permit a simpler interface unit design and to permit a "looser" more tolerant system operation.

The control-law or applications software was specified to be independent of the multicomputer structure, with the redundant hardware transparent to application routines.

Finally, overall system characteristics were specified. The digital system was to operate full-time and in fact be the primary (albeit experimental) flight-control system of the airplane. It would be used during the first takeoff and landing. The flight-critical system was to be given full surface authority in all three axes. The mechanical system had already been removed during the first phase of the F-8 DFBW program. It would not be available. These requirements meant that the primary system would have to be fully man-rated and flight qualified prior to the first flight.

System Description[18,19]

The basic system configuration is shown in Figure B.5. The major components of the F-8 DFBW system are:

(1) Digital Computers (3) (see Figure B.6).

(2) Interface Unit (IFU) (3 independent sections in one chassis) (shown with the computers in Figure B.7).

(3) Sensor Pallet (3 rate gyros on each axis and 3 accelerometers on each axis for a total of 18 sensors) (see Figure B.8).

(4) Additional Sensors (2 heading and attitude systems, 2 angle-of-attack sensors, 1 slideslip sensor, and 3 sensors for each pilot control).

(5) Cockpit Control and Display (Encoder/Decoder, Mode and Gain Panel, Annunciator Panel, Digital Autopilot Panel, and Computer Input Panel) (see Figure B.9).

(6) Computer Bypass and Servo Electronics System (3 Bypass and Servo Electronics (BASE) units and 1 status/engage panel) (see Figure B.10).

(7) Secondary Actuators (5 including right and left aileron, right and left elevator, and rudder) (see Figure B.11).

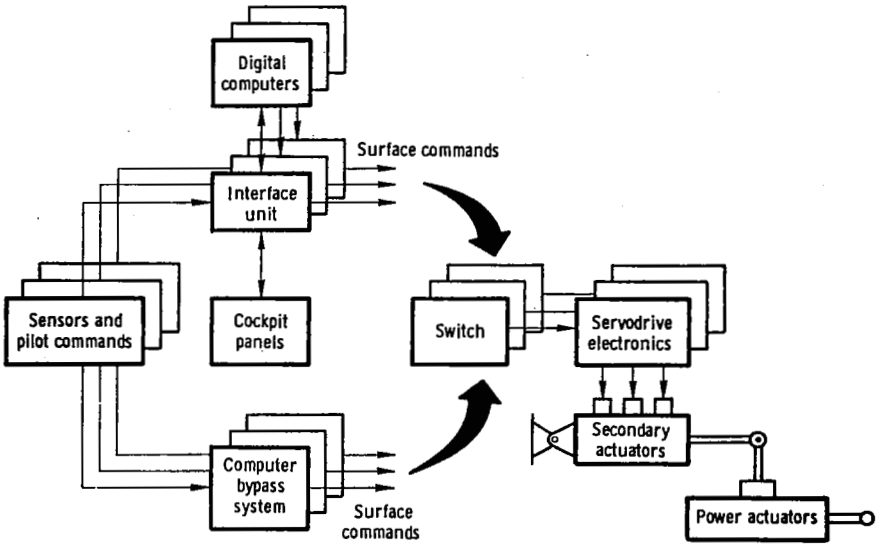


Figure B.5. F-8 DFBW control system mechanization.

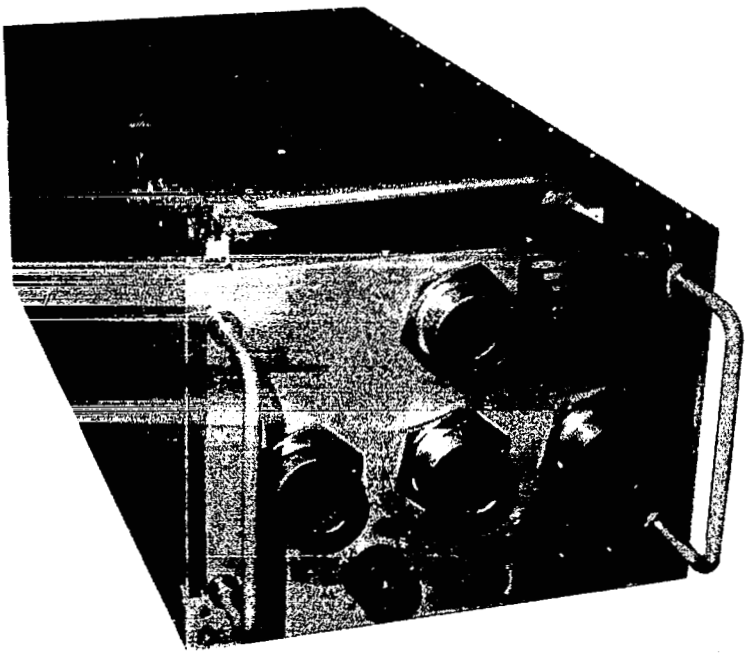


Figure B.6. Central processor unit.

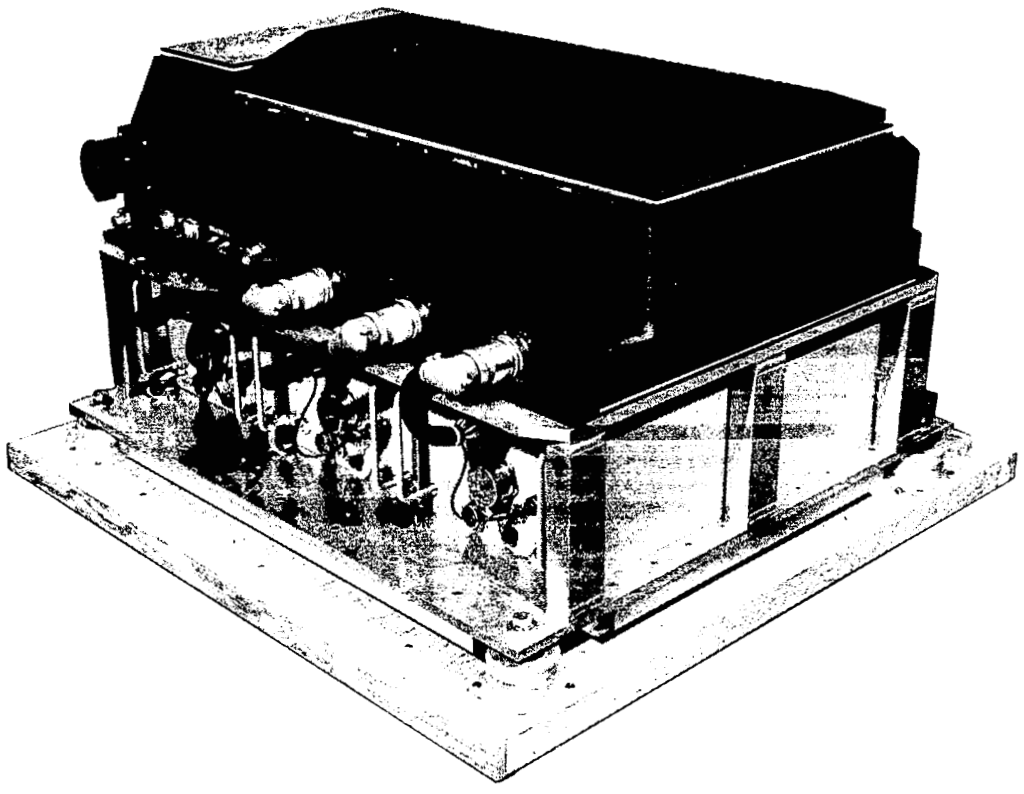


Figure B.7. Pallet assembly containing the interface unit and three central processors.

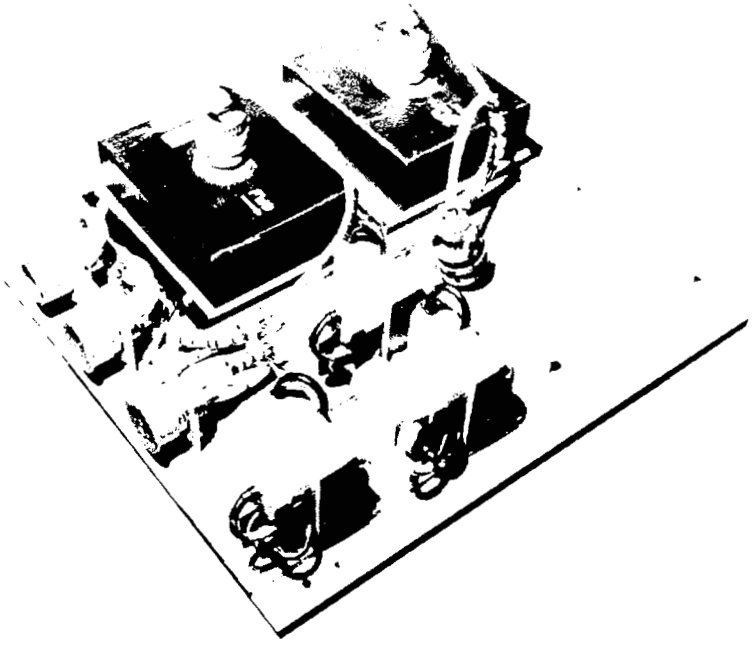


Figure B.8. Inertial sensor assembly.

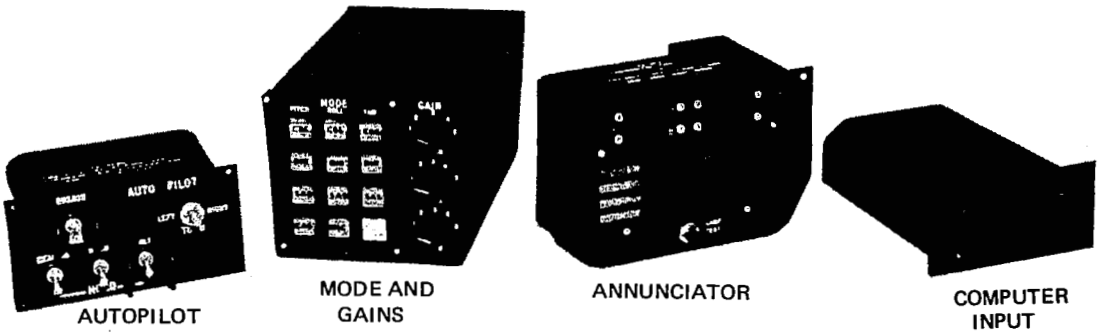


Figure B.9. Cockpit panels.

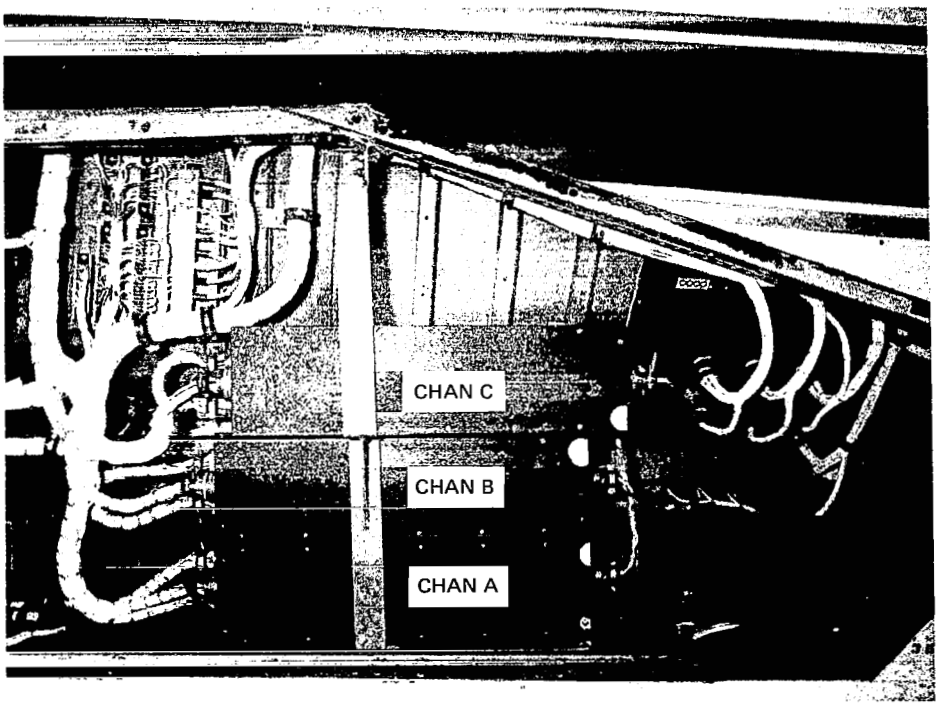


Figure B.10. Computer bypass and servo electronics system installed in airplane.

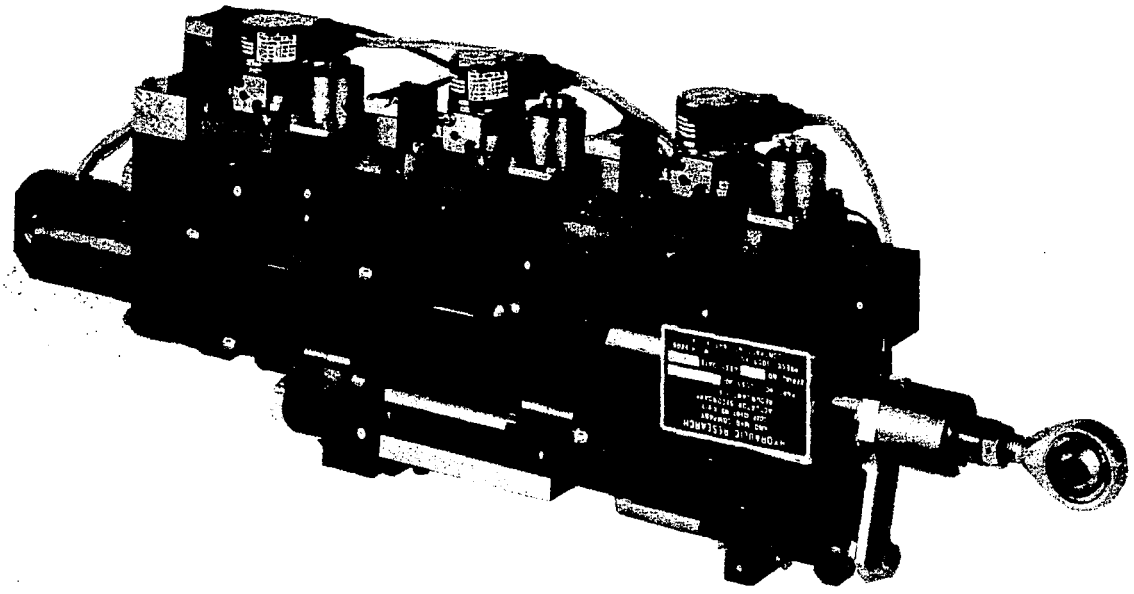


Figure B.11. Triplex secondary servo-actuator assembly.

These major components are briefly described to give an understanding of the basic characteristics and operation of each unit. The physical installation of this equipment in the aircraft is then outlined, and the overall operation of the system is described. Particular emphasis is placed on the failure-detection and redundancy management techniques.

DFBW F-8 Major Components

Computer. - The AP-101 computer used in the F-8 DFBW is similar to that used in the Space Shuttle. This computer was developed over the 1972-1973 time period. It is a general-purpose stored-program parallel machine. It works with both 16- and 32-bit words. It has a microprogrammed instruction set with 146 total instructions, which include both fixed-point and floating-point operations. The AP-101 uses a magnetic-core memory with 32,768 36-bit words. The words include two parity bits and two store protect bits. The AP-101 is basically one full ATR (19.3 × 25.6 × 49.8 cm) and weighs 26 kg. Its primary power is 28 Vdc and it uses 375 watts; it is cooled by individual blowers.

Interface unit (IFU). - The IFU contains the equipment necessary to process and condition the I/O signals for the three digital flight computers. The IFU was specially designed and built for the F-8 DFBW program. There are actually three electrically independent IFU channels,

one for each processor. Because of F-8C installation requirements, the three channels are packaged within a single enclosure. Each IFU channel is interfaced with only the one processor, and can be thought of logically as part of the processor.

Each IFU channel is responsible for four major functions:

(1) To provide conditioning of input signals, convert the analog signals to digital form, and provide buffer memory for input data.

(2) To process output signals and perform digital-to-analog conversions.

(3) To provide for interchannel data transfer between computers.

(4) To participate in fail detection and redundancy management.

A functional diagram of the IFU is shown in Figure B.12. A diagram showing the way sensor data is processed and transferred between channels is shown in Figure B.13.

Sensors. - There is a sensor pallet that was assembled and installed in the aircraft specifically for the DFBW system. The DFBW system also uses several other aircraft sensors.

The sensor pallet consists of nine gyros and nine accelerometers. There are three gyro assemblies, with three gyros in each assembly. Each gyro in an assembly is mounted parallel to one major aircraft axis. The arrangement for the accelerometers is the same as for the gyros.

The DFBW system also uses several other sensors, which are distributed about the aircraft. There are triple-linear-variable-differential-transformer (LVDT) stick-position sensors for both roll and pitch control and also triple-LVDT sensors for the rudder pedals. There is also an experimental side-stick controller. Thus, there are triple-LVDT force sensors for both roll and pitch from the side stick. The system receives inputs from two angle-of-attack sensors and one sideslip sensor. Two heading and attitude reference systems are used in the system. Each provides three synchro signals: one for pitch, one for roll, and one for heading. Mach inputs are obtained as dc signals from two Mach meters. Altitude is obtained as serial digital signals from two altimeters.

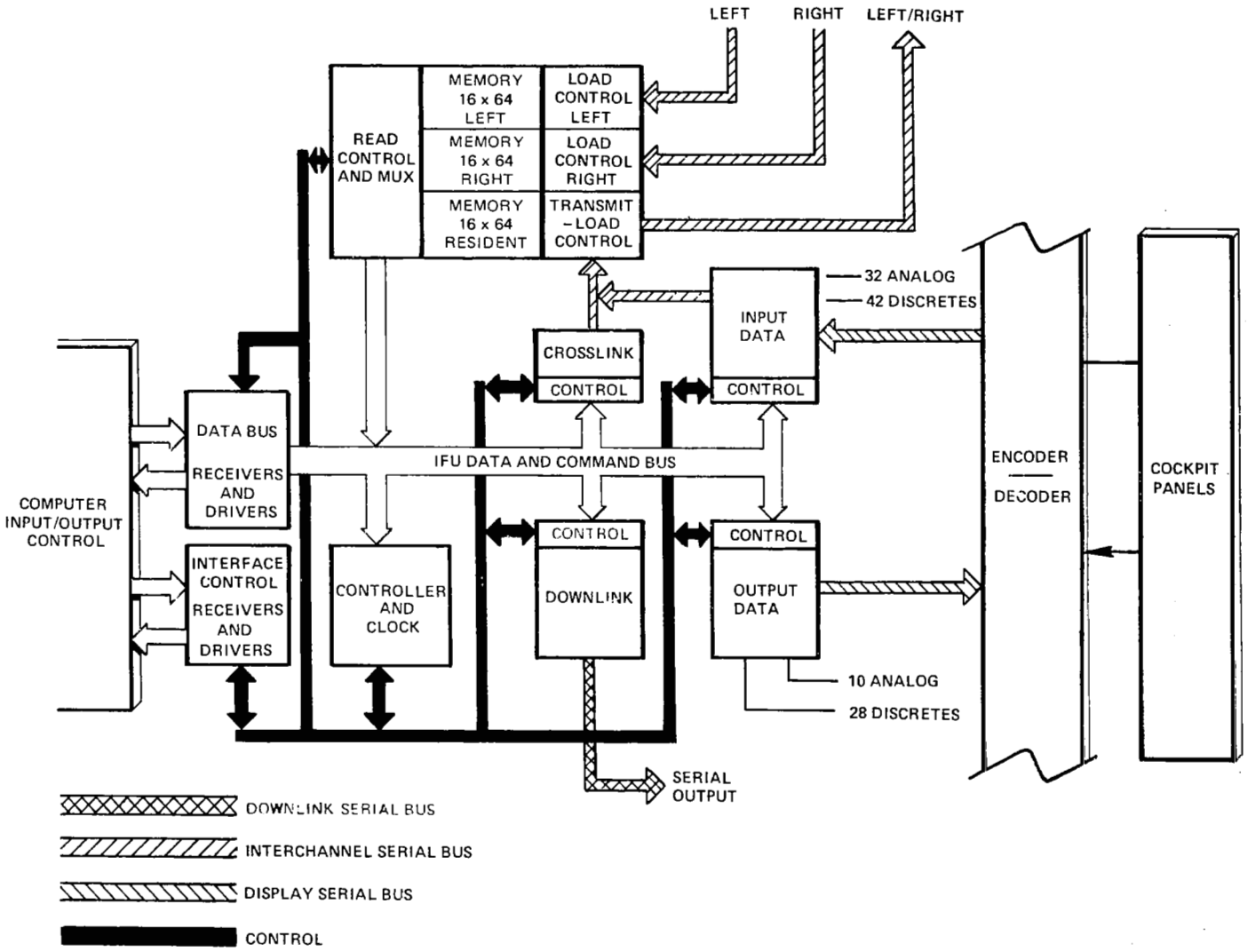


Figure B.12. IFU simplified functional diagram.

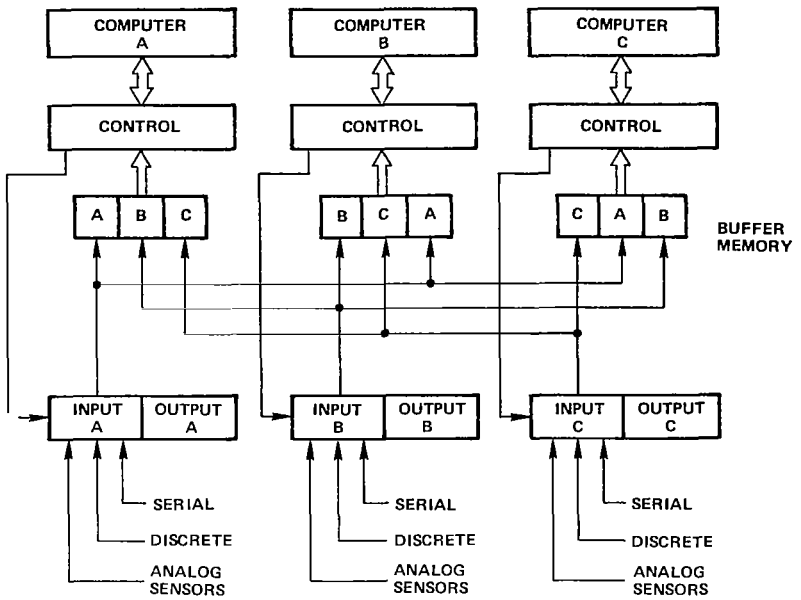


Figure B.13. Input.

There are also position sensors on the control surfaces, the horizontal stabilizer actuator, and the wing.

Pilot control and display. - The F-8 DFBW has four pilot control and display panels. These units allow adequate visibility and flexibility in an experimental system. Many of the functions would not be necessary or desired on a production system. Each of the panels is interfaced to the IFU and computers by the encoder/decoder unit.

Mode and gain panel (see Figure B.9): The Mode and Gain Panel provides control of the major modes of the system and allows pilot control of selected parameters. There are separate mode controls for each channel: roll, pitch, and yaw. These mode switches allow manual switching between the digital and analog systems. With the digital system there is also the choice between the Direct Mode and augmented modes. The Direct Mode gives a direct connection between the pilot controls and the aerodynamic control surfaces.

In the pitch channel, there is simple stability-augmentation (SAS) mode and a more highly augmented command-augmentation (CAS) mode. There are also lateral-direction SAS modes. The mode switches are lighted to indicate which mode is active. These lights indicate the mode both when it is manually selected or when it changes automatically due to system-detected faults.

Digital autopilot panel (see Figure B.9): The Digital Autopilot Panel is very similar to traditional autopilot control panels. It has a magnetically latched engage switch and mode switches for altitude hold, Mach hold, and heading. It also has a turn control switch.

Annunciator panel (see Figure B.9): The Annunciator Panel is capable of displaying 20 separate indications; four of the indicators have a switch for reset. These displays include:

(1) Hardware-Detected Failures: Channel A Fail, Channel B Fail, Channel C Fail.

(2) Software-Detected Resettable Failures: Trim, Downmode, Self-Test.

(3) Status and Software Detected Failures: A Temp, B Temp, C Temp, P RAV, R RAV, Y RAV, Flap, Air Data, Alpha, Center Stick, Side Stick, Rudder Pedal.

Computer input panel (see Figure B.9): The Computer Input Panel allows the pilot to initiate preprogrammed software functions. These include the control of an extensive preflight test program. In flight, control-system options can also be selected. The panel has two thumbwheel switches to select the program. The selected program is displayed on a three-digit display. The program is initiated when the Enter button is pressed.

Encoder/decoder unit. - The Encoder/Decoder Unit provides the interface between the control and display panels and the IFU. Although housed in one chassis, the unit contains independent channels for failure protection.

Computer bypass and servo electronics system (CBS).[20] - The CBS consists of three parallel Bypass and Servo Electronics (BASE) units and a status/engage panel. A diagram of the BASE unit is shown in Figure B.14. It contains analog circuits for input signal conditioning of the surface commands from the digital system and for direct input of pilot-control position sensors for the computer bypass circuit. It also contains switches to select either the digital or bypass commands. The selected commands from each unit are crosswired into midvalue-select circuits. A comparison monitor between the midvalue selected and the local channel command is used for fault detection. The BASE unit also contains all the electronics necessary both to close the servo loop on the actuators using a posision feedback signal and to process the delta pressure (Δp) signals from the actuator used for equalization and fault detection.

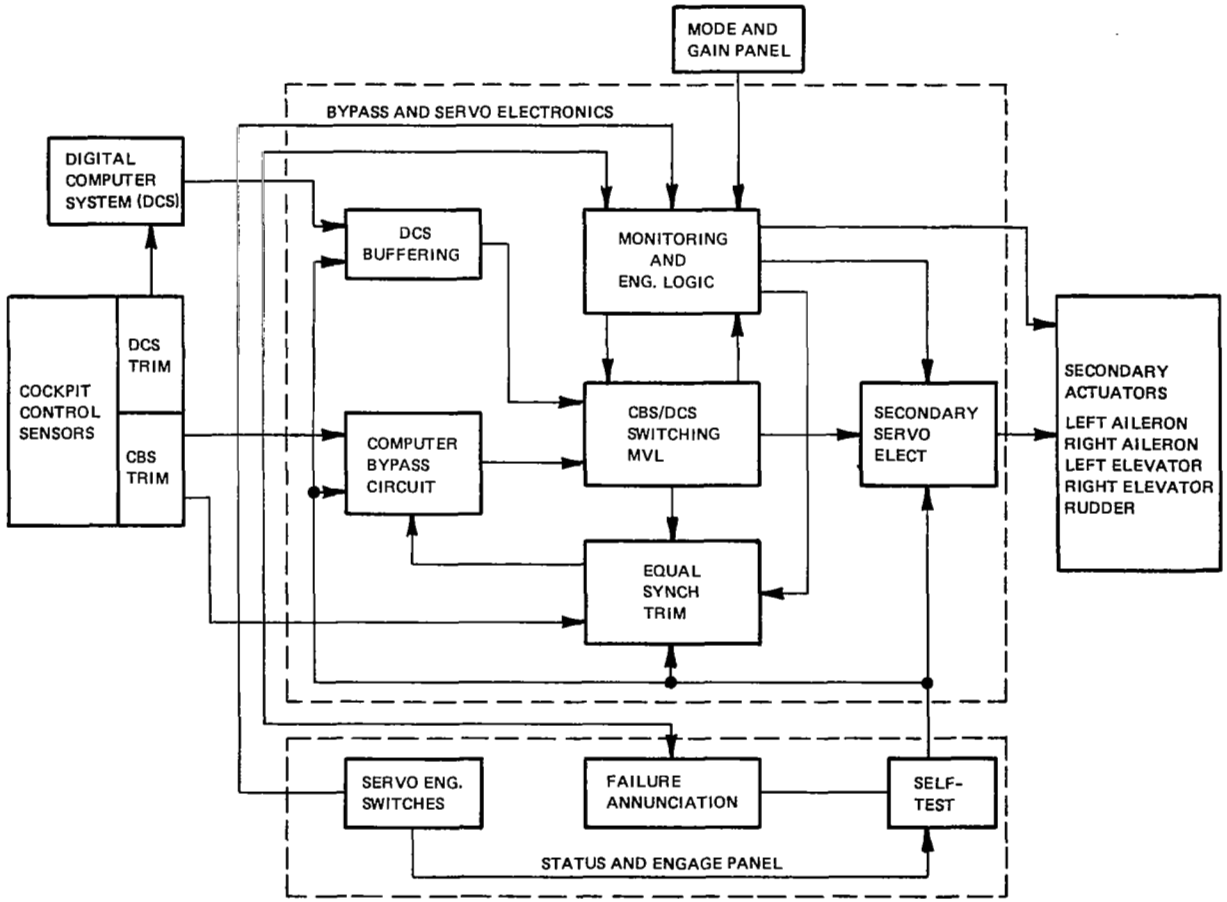


Figure B.14. Simplified F-8 DFBW computer bypass and servo electronics system block diagram.

The BASE unit contains discrete logic circuits which implement much of the fault detection and redundancy management for the final test of the digital commands, the bypass circuits, the servo electronics, the actuators, and the electrical power.

The status/engage panel shown in Figure B.15 provides engage switches for each channel of each actuator (15 in all). Each actuator can be in the OFF, AUTO, or MANUAL mode. The normal mode is AUTO, which allows automatic engagement and redundancy management by the system. The first channel switched to the MANUAL mode is operated as a dedicated single-channel system and the other two channels are locked out. This feature was originally intended for preflight diagnostic purposes, but also serves as a "last resort" configuration in the event of loss of two analog channels. The status/engage panel also contains the control for extensive self-test of the CBS system.

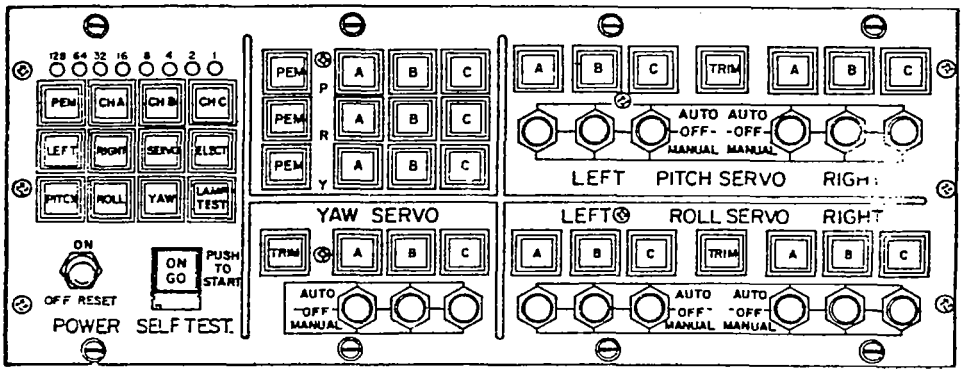


Figure B.15. Status/engage panel.

Secondary actuator. - The secondary actuator is triply redundant and is capable of providing a single fail-operational/fail-neutral force-sharing operation for any two similar nonsimultaneous failures. The actuator has three independent electrohydraulic channels. Each channel incorporates the following features and components:

(1) Independent hydraulic fluid supply.

(2) Two-stage electrohydraulic flapper nozzle servo valve to control the actuator motion.

(3) Solenoid valve to port pressurized fluid to the servo valve and to the actuator chambers.

(4) Engage valve, which by being engaged (energizing of the solenoid valve) allows the servo valve to port pressure into the actuator chambers, and by being disengaged (de-energizing of the solenoid valve) puts the actuator into a bypass mode preventing hydraulic lock.

(5) Pressure transducer for Δp sensing, failure detection, and channel synchronization.

(6) LVDT for position output sensing and feedback-loop closure.

A schematic diagram of the servo actuator is shown in Figure B.16 and a more detailed schematic of the electrohydraulic servo valve is shown in Figure B.17.

The servo actuator has been designed to assure that all failures are detected and that no single failure will cause hydraulic lock. Any passive failure in the electrohydraulic servo valve is detected by the fact that a null bias is built into the valve's first stage. A current of 10 percent of full value is required to hold the valve at null. If there is any failure in the coil or electrical connections, the null is not held and a Δp is generated which is detected in the servo electronics and causes the channel to be shut off. The system "ON" solenoid is electrically fail-safe. If there is any electrical or coil failure, the valve will shut, disabling that channel to a passive condition. If there is a mechanical failure, such as a broken spring, the valve could remain open when it should be closed because of some other failure. However, the actuator will still operate, though with reduced performance, because the other two channels can overcome any irregularity in the failed channel. Moreover, experience shows that this kind of mechanical failure is extremely rare.

Hydraulic lock is normally prevented by the engage valve. When the engage solenoid shuts off hydraulic pressure or pressure is lost for any other reason, the engage valve is moved by a spring to the bypass condition. If the spring in the engage valve breaks, the channel could be locked by the electrohydraulic servo valve also being at null. This condition is prevented because the second-stage servo valve is also spring biased; if hydraulic pressure is lost, this valve will move hard over and prevent lock.

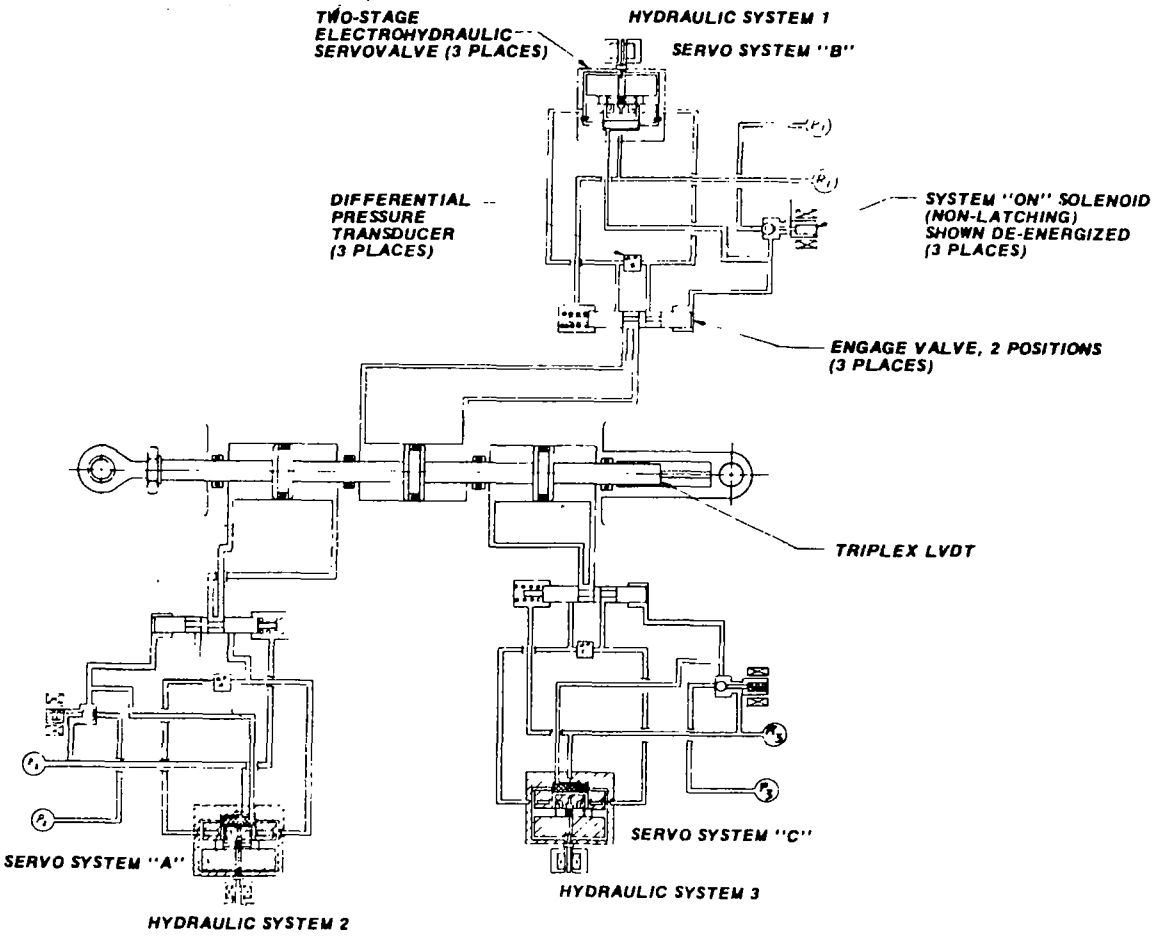


Figure B.16. Phase II hydraulic schematic, triplex redundant secondary servoactuator.

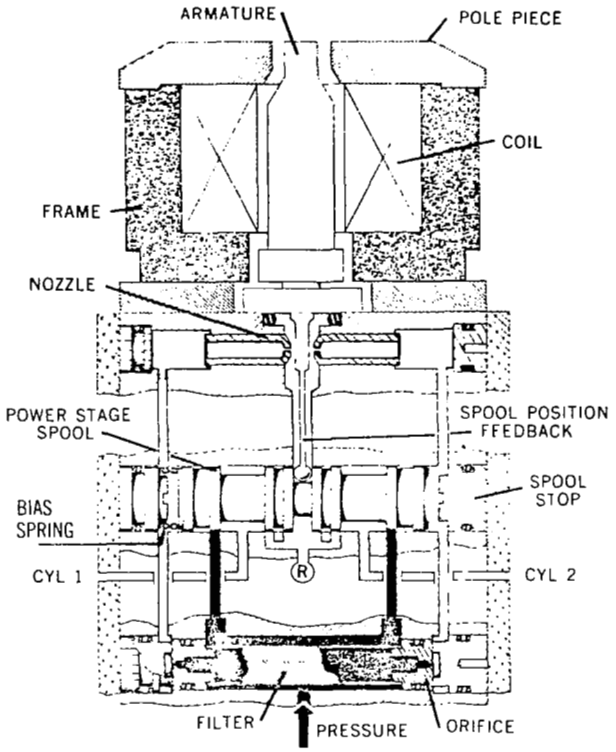


Figure B.17. Phase II two-stage electrohydraulic servo valve.

Installation

The Phase II DFBW system is installed in a Navy F-8C aircraft, which is single engine and single seat, and is capable of supersonic flight. It has a two-position variable incidence wing for reducing fuselage attitude during the landing approach. The modifications to the aircraft for this program were all internal; there were no basic structural or aerodynamic changes. The major change was the removal of the mechanical control linkages. The only other changes were the addition of the flight-control sensors, electronics, and actuators.

The location of the major elements of the system is shown in Figure B.18. The three computers and the IFU are mounted on a pallet that was shown in Figure B.7. The pallet is installed just behind the cockpit at the top of the fuselage. The computer bypass and servo drive electronics are mounted in the lower left side of the fuselage behind the cockpit. The encoder/decoder unit is mounted in the nose to minimize the wire run lengths. The gyro and accelerometer sensor pallet is located

near the center of gravity in the belly of the aircraft. The angle-of-attack and sideslip sensors are located on a boom in the front of the aircraft. The secondary actuators are located with the primary actuators and essentially connect to the same position as the original mechanical linkage.

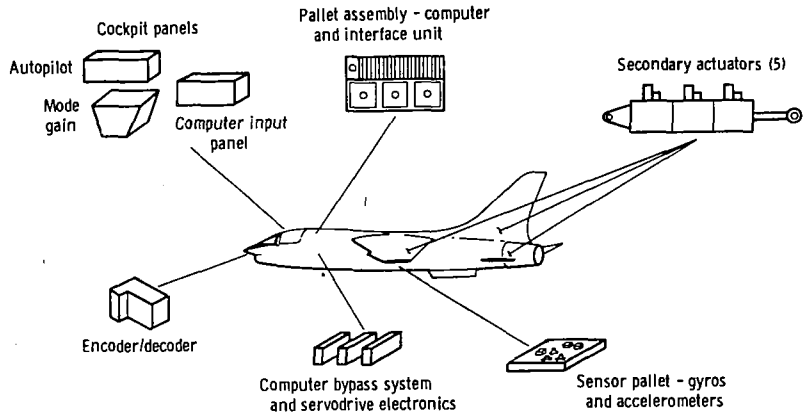


Figure B.18. F-8 DFBW hardware elements.

Electrical power to the flight-control system is obtained from three independent buses, which are supplied by a dedicated engine-driven dc generator. Each bus is backed up by a 40-ampere-hour battery. These batteries can power the full digital system for 60 minutes in the event of a generator failure. The batteries are isolated from each other by diodes and circuit breakers and supply power whenever their voltage exceeds the voltage on the buses. A battery is always on an individual bus with no switching involved. The flight-control system is not connected to the existing aircraft power systems except for ac power, which is needed for the computer and pallet blowers and attitude and Mach sensors. A ram air turbine can be deployed if necessary to supply emergency ac power for the blowers. There is an inverter in each channel that supplies 26-volt 400-Hz power for the pilot-control input sensors and the actuator position feedback signal sensors.

Three separate hydraulic power supplies are used for the three channels of the secondary actuators. Two of these are the existing system for the two channels of the primary power actuators. The third is the utility system used for landing gear, speed brakes, etc. One of the hydraulic systems can be powered in emergencies by the ram air turbine.

System Operation

A diagram of the total system was given in Figure 9. The primary means of flight control is through the triplex digital system. This system is responsible for:

(1) Fault detection and redundancy management of the computers themselves and their associated IFUs.

(2) Data processing, fault detection, and redundancy management of the input sensors.

(3) Computation of the appropriate control-law algorithm.

(4) Production of the four necessary analog surface position commands.

The BASE units are responsible for:

(1) Midvalue selection and comparison monitoring of the surface commands from the digital system.

(2) Signal conditioning, fault detection, and redundancy management of the analog backup computer bypass channel.

(3) Switching from primary digital commands to bypass commands.

(4) Closing the servo loop, fault detection, and redundancy management of the actuators.

(5) Fault detection and redundancy management of the electrical power.

The redundancy management of the hydraulic power is manual.

The following subsections describe the software in the digital system, the fault detection and synchronization of the computers, the sensor data processing and redundancy management, and the operation of the BASE system.

Software organization. - The approximate memory allocations for the major program elements are shown in Figure B.19. The software is executed as a sequence of minor cycles, which are initiated by a timer interrupt generated within the computer, causing the program to stop doing whatever it was doing and begin executing the basic minor-loop program. The nominal time period for the minor loop is 20 milliseconds. This time can be varied for experimental purposes; however, most of the basic program functions are performed within 20 milliseconds. Some outer-loop control computations are partially performed within each minor cycle so that the whole function is completed in an integral number of minor cycles, forming a major cycle. The sequence of execution of the program elements is given in Figure B.20.

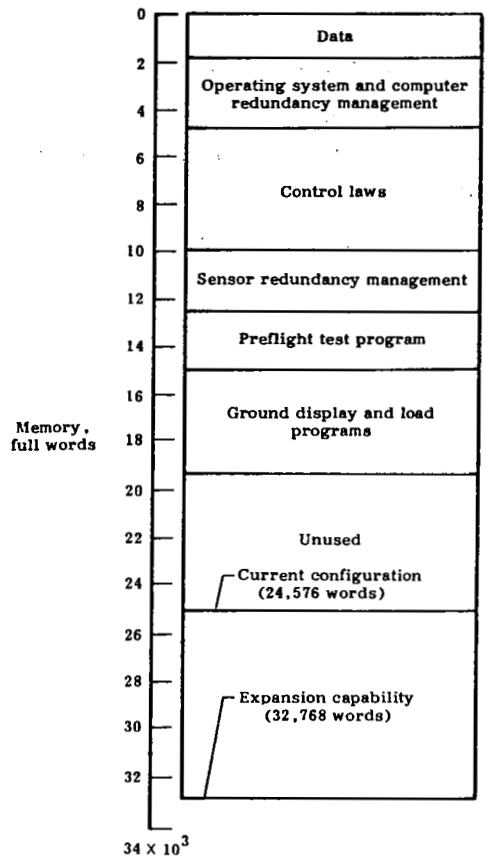


Figure B.19. Software memory allocation.

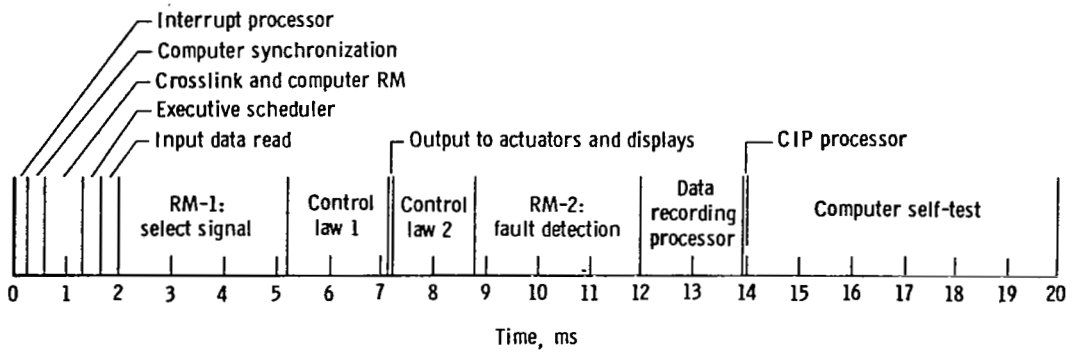


Figure B.20. Software sequence and timing during one minor cycle: three channels, direct modes.

Computer fault detection and synchronization. - The first step in ensuring the proper operation of a digital-processor-based flight-control system is to assure that the computers are working properly. Once full confidence can be placed in the computers, their significant processing power can be used to monitor faults in the rest of the system.

Fault detection can be divided into two different categories. One is self-test, where a unit performs tests to determine its own health. The other category involves monitoring or testing by other units. Fault detection in both of these categories is performed in a hierarchy of different levels. Faults are detected on as low a level as possible. However, for faults that cannot be detected on a low level and for protection against any failure of the lower level techniques, higher level tests are used. The total set of tests is designed so that each test complements the others; together, the tests are able to cover the entire system and assure the required level of system integrity.

The computers in the F-8 DFBW system are tested at several levels by both self-testing and external monitoring. These tests are performed both by special hardware and software.

Self-test: Each computer/IFU channel determines its own condition by using hardware built-in test equipment (BITE) and by software self-test programs. The computer BITE detects faults in the execution of instructions, loss of power, parity errors in memory, and failure of a go/no-go counter to be reset. The go/no-go counter is reset by a software command. Thus, this test will detect any kind of hardware or software problem that will keep the program from completing its basic computation cycle in the proper time. Problems detected by this test include the program getting caught in a continuous loop or branching to the wrong part of the memory.

The BITE in the IFU channel tests for timeout, oscillator failure, and power failure. The timeout assures that the IFU performs its basic operations within certain maximum time limits.

There are two categories of response to the detection of a BITE fault. Certain faults such as loss of power are potentially transient, and it is desirable to attempt to regain normal operation. This is achieved by requesting a restart, which will be discussed later. Because other faults are considered to be permanent, a signal is generated to declare permanent failure of a channel.

The other methods used by the computer for determining its own health are self-test software routines. There are two self-test routines. One routine is continually run during flight. The other routine is run only after an initial program load of the computers. This routine includes all flight tests plus certain other tests that could not be performed during normal operation without disrupting normal operation. These routines are designed to test the central processor unit and memory functions with a detection error confidence of 95 percent.

The computer/IFU channel also uses special circuits in conjunction with software programs to test the input and output interfaces. The analog command signal, certain discrete bits, and bits within the serial data words going to the encoder/decoder are wired back into the computer. Software routines in the computer check these wrap-around inputs and compare them with what the output should have been. This test checks the critical output interface hardware and a majority of the input interface hardware.

Synchronization: The hardware and software self-test monitors in each computer/IFU channel will detect the majority of all possible failures, and, if a failure is detected, will produce a signal causing that channel to be disregarded. It is now possible to connect the three computers together so that they can monitor each other to detect faults that may not be caught by the hardware and software self-test. The first step toward achieving simultaneous operation of the computers in the F-8 DFBW system is to synchronize them so that they are performing the same operations at very nearly the same time. Synchronization is necessary to cause data to be read from the sensors at the same time, allowing fault detection by comparison of redundant sensors. The synchronization of computations is also important to allow comparison of the analog command outputs from the computer. This comparison is performed in the BASE analog electronics.

Another important task performed by the synchronization is computer fault detection. One of the best ways for each computer to determine the health of the other two is by their ability to come into synchronization. The computers are synchronized by a program in each computer, which sends discrete signals to each of the other two computers (Figure B.21). The computers are synchronized when the program reads and verifies the discretes it has received from the other computers. If, after a short wait to allow for skew between processors, one computer

fails to synchronize with the other two, the two remaining computers exit the sync program and continue normal processing. This synchronization occurs only at the beginning of each minor cycle. These 20-millisecond cycles are begun within 10 to 50 microseconds of each other.

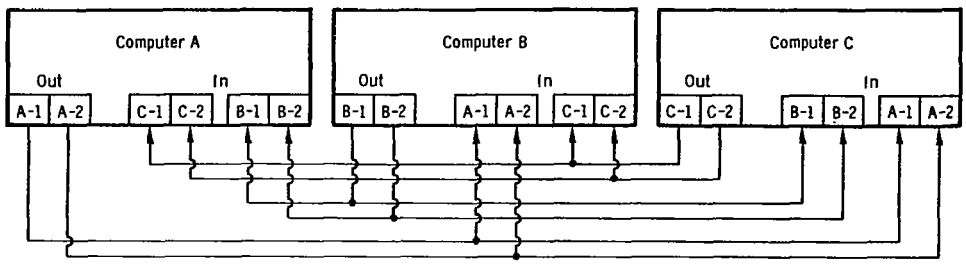


Figure B.21. Synchronization discretes.

Cross-channel monitoring: If the computers can be successfully synchronized, the next step in their monitoring of each other is to transfer data among themselves. This transfer is done through the buffer memories in each IFU channel, and consists of six data words. The transferred data includes an identification of the computer channel, the computer's minor cycle count, the mode it is in, and its assessment of the failure status of the other two computers. Failure to receive data from a synchronized computer for 10 successive cycles results in a "hard fail" declaration and that computer cannot be used again. Failure to receive data from a nonsynchronized computer results in the declaration of a "soft fail" and enables inclusion of this computer in the operating set when its sync discretes and data appear. If a computer's data is not properly identified for 10 successive cycles, a hard fail is declared. If a computer's cycle count and mode do not agree with those of the other two computers, it requests a restart.

Restart: Restart is requested by a computer for a number of reasons including:

(1) Freshstart—initial power up.

(2) Power disruption.

(3) Crosslink fail—I/O or data.

(4) Software program and/or computer BITE detected errors.

Whenever a restart is requested, the three computers, by way of the crosslink, exchange enough data to guarantee that they are in agreement. This transmission includes the choice of the computer considered to have valid data and the data to be used by the offending computer. The data exchanged is 94 16-bit words, and includes such items as sensor and discrete failure history and control-law parameters.

To prevent continuous restart requests caused by a failure in the system, each computer maintains a count of all restart requests. If the number of restart requests made by any computer exceeds a prescribed tolerance, that computer is declared hard failed and its requests are subsequently ignored. The entire restart process takes approximately 8 milliseconds from recognition of request to resynchronization.

Failure voting: It is necessary for two computers to agree before a third can be declared failed. If the self-test software or hardware in a channel declares itself failed, that channel is inhibited from voting on the other computers. A logical diagram of the hardware within an IFU channel that implements this process is shown in Figure B.22. The output signal which declares a channel failed is sent to the BASE and causes that channel to switch to the analog channel.

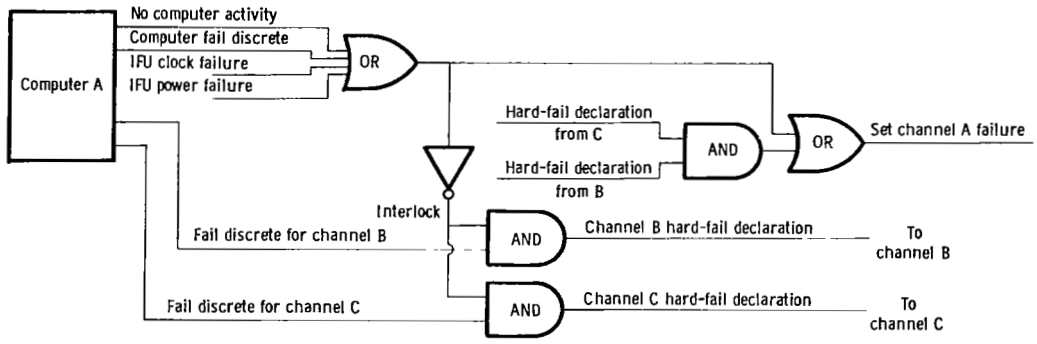


Figure B.22. Functional diagram of fault detection hardware in IFU (shown for channel A).

Sensor data processing and redundancy management. - The data from all redundant sensors is available to each computer. The data is processed by redundancy management (RM) programs, which are performed in two phases. The only function of the first phase is to obtain the best estimate of the actual parameter value based on the available multiple sensor inputs, and provide this data for use in the control-law computations. The second phase performs fault detection and identification, and controls the reconfiguration of the select logic used in the first phase.

A typical triplex RM algorithm is shown in Figure B.23. The first phase begins as a midvalue select mode, changes to an averaging algorithm after the first hard failure, and finally degrades to a default output value after the second failure. A hard-sensor fault is declared by the second phase when a sensor differs from the selected value by an amount greater than the allowable tolerance for a given number (N) of consecutive passes. Failure-status logic monitors the results of the tracking test and, through hard-fail flags, causes the mode or function using that sensor to be inhibited. For example, should the entire roll-rate-gyro set be lost, the roll stability augmentation system (SAS) would be inhibited. In some cases, annunciation is given to the pilot when an entire sensor set has been lost. The first failures of sensors in a triplex set are not annunciated to the pilot.

Operation of the BASE units. - Each BASE unit receives the four analog surface position commands from a corresponding digital channel (refer to Figure 9). The unit also receives a valid discrete (Figure B.22) from all three channels. If two of the three digital channels have valid discretes and have valid surface commands, the primary digital mode can be engaged using the Mode and Gain Panel. This mode puts digital/bypass switches corresponding to each actuator in the digital position. There are five of these circuits in each unit for left and right elevator, left and right aileron, and rudder. A typical circuit is shown in Figure B.24. The switch outputs go to a midvalue select circuit in that channel and are also cross-wired to the other two channels. The selected midvalue is fed back into the bypass system to provide synchronization so that if the digital/bypass switch is charged, there will be no transient.

The selected midvalue is compared with the signal from that channel. If the difference exceeds a set value, the corresponding

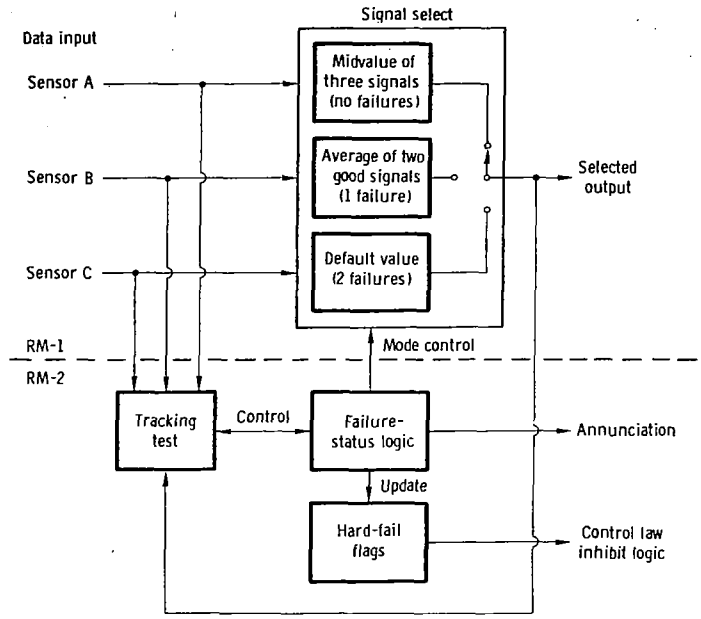


Figure B.23. Triplex analog sensor redundancy management algorithm.

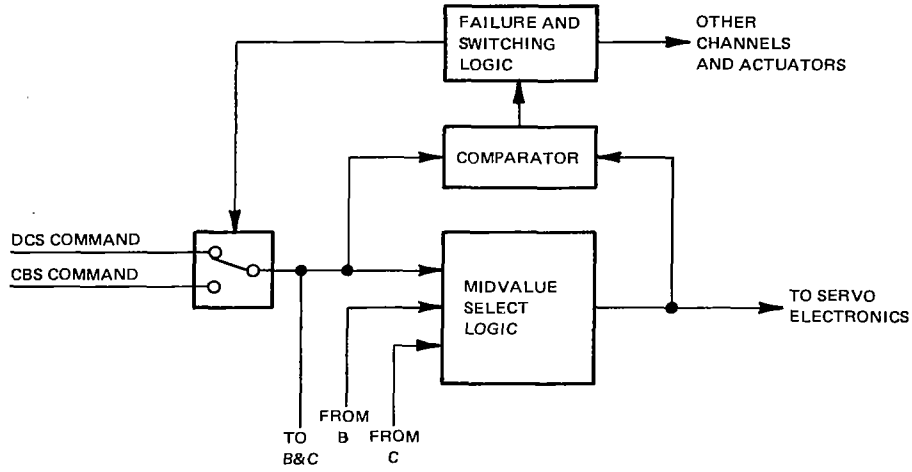


Figure B.24. BASE switching and selection logic.

switch is charged to the bypass position. The synchronization process is still active so that the switched channel follows the signals from the other two channels that are still operating. The results of the comparison are also cross-wired to the other two channels. If the comparison fails on two of the three channels for 40 milliseconds, all channels of that axis are switched to bypass, and synchronization is disabled. The BASE units also switch all axes of all channels to bypass if two of the three valid discretes from the digital channels are lost for 40 milliseconds. In the bypass mode, the comparitors and voters are still active so that if two of three comparisons fail in any actuator channel, that channel is disabled.

The output from the midvalue select circuit goes to the actuator control electronics as shown in Figure B.25. The actuator is controlled by a servo loop using a shaft-position feedback signal from an LVDT. The signal from a Δp transducer across the actuator piston for that channel is also fed back along with the Δp's from the other two channels. These Δp's are fed into a midvalue-select circuit. The midvalue selected is fed back into the servo loop as an equalization signal to minimize the low-frequency force fight that can occur in high-pressure-gain systems as a result of slight trim mismatches.

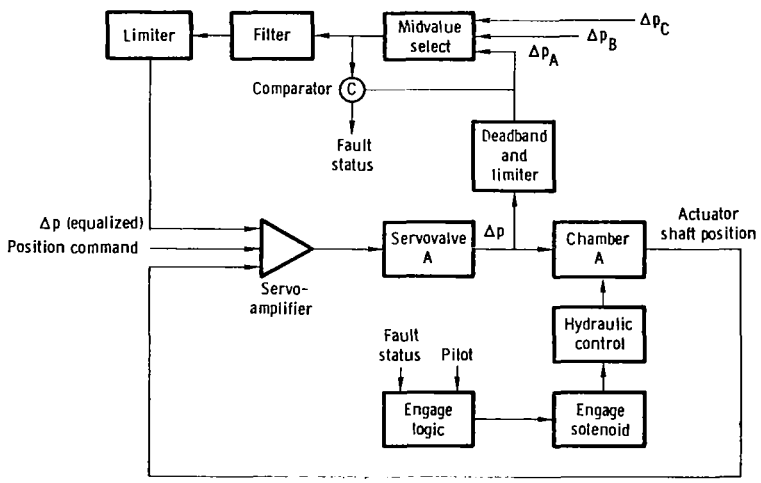


Figure B.25. Schematic diagram of single channel of secondary actuator and servo electronics.

The selected midvalue of Δp is also compared with the value for that channel. If it is outside a set limit, the engage solenoid is disabled, supply pressure is dumped to return, and a bypass path around the piston in the failed channel is opened. Faults are annunciated in the cockpit, and reset capability is provided to the pilot. A second failure in the same actuator causes that actuator to be turned off. Mechanical centering springs move the disabled actuator to a safe static position. The Δp comparison limits are set to be relatively wide. A passive failure may not be detected, particularly if the good Δp's are small due to small control commands. Hardover faults will be detected, however.

Each BASE unit also contains power-monitoring circuits for its own power supply, and thus also for the input dc and ac power supplies. A power-supply failure will disable that channel. The power monitor signals are also cross-connected to the other two channels. If failures are detected in two of the three channels, the remaining good channel is forced into single-channel operation, and the two out of three voters are disabled. Any actuator channel can also be put into single-channel operation by the MANUAL switch position, which also disables two out of three voters.

APPENDIX C

ACRONYMS

ARM	analytical redundancy management
ATR	air transport racking
BASE	bypass and servo electronics
BITE	built-in test equipment
CARSRA	computer-aided redundant system reliability analysis
CAS	command augmentation system
CAST	complementary analytic simulation technique
CBE	common BASE electronics
CBS	computer bypass (and servo electronics) system
CIP	computer input panel
CPU	central processing unit
DADS	digital air data system
D/A	digital-to-analog
DCS	digital computer software; digital computer system
DFBW	digital fly-by-wire
DFCS	digital flight-control system
DFRC	Dryden Flight Research Center
DG	directional gyro
FAR	Federal Aviation Regulations
FDL	Flight Dynamics Laboratory
FIFO	first-in/first-out
FMEA	failure modes and effects analysis
FMET	failure modes and effects test
FTMP	fault tolerant multiprocessor
IFU	interface unit
ILS	instrument landing system
I/O	input/output
JSC	Johnson Space Center

LARC	Langley Research Center
LCL	lower confidence limit
LPA	left pitch actuation
LRA	left roll actuation
LVDT	linear variable differential transformer
MDR	maneuver drag reduction
MPX	multiplexer
MTBF	mean time between failure
MVL	middle value logic
MVS	midvalue select
NAMSO	Navy Maintenance Support Office
NASA	National Aeronautics and Space Administration
OAST	Office of Aeronautics and Space Technology
PDS	primary digital system
PIND	particle-induced noise testing
QA	quality assurance
QMR	quadruple modular redundancy
RAV	remote augmentation vehicle; remotely augmented vehicle
R/A	radio altitude
RM	redundancy management
RPA	right pitch actuation
RRA	right roll actuation
SAS	stability augmentation system
TMR	triple modular redundancy
UCL	upper confidence limit
VG	vertical gyro
YA	yaw actuation

REFERENCES

1. Conn, R.B.; Merryman, P.M.; and Whitelaw, K.L.: CAST - A Complementary Analytic-Simulative Technique for Modeling Complex, Fault-Tolerant Computing Systems. Integrity in Electronic Flight Control Systems, AGARDograph 224, 1977.

2. Bjurman, B.E., et al.: Airborne Advanced Reconfigurable Computer System (ARCS). Prepared by Boeing for NASA, NASA CR-145024, August 1976.

3. Mathur, F.P.: Reliability estimation procedures and CARE: The computer-aided reliability estimation program. Jet Propul. Lab. Quart. Tech. Rev., vol. 1, October 1971.

4. Reliability Model Derivation of a Fault-Tolerant, Dual, Spare-Switching, Digital Computer System, Final Report. Raytheon Report ER74-4108, March 1974.

5. Stiffler, J.J.: Computer-Aided Reliability Estimation. Presented at AIAA 1st Computer in Aerospace Conference, Los Angeles, 30 October to 1 November 1977.

6. Fault/Failure Analysis Procedure. Society of Automative Engineers Aerospace Recommended Practice, ARP-926, November 1978.

7. Reliability Prediction of Electronic Equipment. MIL-HDBK-217C, 9 April 1979.

8. Green, A.E.; and Bourne, A.J.: Reliability Technology. Wiley-Interscience, 1972.

9. Nonelectronic Parts Reliability Data. Reliability Analysis Center, Rome Air Development Center, NPRD-1, Summer 1978.

10. Revision of RADC Nonelectronic Reliability Notebook. Prepared by Martin Marietta Aerospace for Rome Air Development Center, RADC-TR-74-268 (RADC-TR-69-458, Section 2), Final Report, October 1974.

11. Special Maintenance Data Report #MDR-0#. Navy Maintenance and Material Management Information System, SAMSO 4790.A2371-01, 20 July 1979.

12. McGough, J., et al.: Digital Flight Control System Redundancy Study. Prepared for Air Force Flight Dynamics Laboratory, AFFDL-TR-74-83, July 1974.

13. Secord, C.L.; and Vaughn, D.K.: Preliminary System Design Study for a Digital Fly-by-Wire Flight Control System for an F-8C Aircraft. Prepared by Honeywell, Inc. for NASA, NASA CR-2609, January 1976.

14. Westermeier, T.F.: Triplex Digital Fly-by-Wire Redundancy Management Techniques. Presented at AIAA Guidance and Control Conference, Palo Alto, Calif., 7-9 August 1978.

15. DeWolf, J.B.; and Wexler, J.: Approaches to Software Verification with Emphasis on Real-Time Applications. Proceedings of AIAA Computer in Aerospace Conference, Los Angeles, Calif., October 1977, pp. 41-51, 545.

16. Rang, E.R., et al.: Digital Flight Control Software Validation Study. Prepared by Honeywell, Inc. for Air Force Flight Dynamics Laboratory, AFFDL-TR-79-3076, June 1979.

17. Szalai, K.J., et al.: Digital Fly-by-Wire Flight Control Validation Experience. NASA TM-72860, December 1978.

18. Szalai, K.J.; Felleman, P.G.; Gera, J.; and Glover, R.D.: Design and Test Experience with a Triply Redundant Digital Fly-by-Wire Control System. Presented at AIAA Guidance and Control Conference, San Diego, Calif., paper 76-1911, 16-18 August 1976.

19. Megna, V.A.; and Szalai, K.J.: Multi-Flight Computer Redundancy Management for Digital Fly-by-Wire Aircraft Control. Presented at IEEE COMCON 77, Washington, D.C., September 1977.

20. Description and Theory of Operation of the Computer By-Pass System for the NASA F-8 Digital Fly-by-Wire Control System. Prepared by Sperry Flight Systems for NASA, NASA CR-144865, May 1978.

TECHNICAL REPORT STANDARD TITLE PAGE

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NASA CR-163110		

4. Title and Subtitle	5. Report Date
RELIABILITY ANALYSIS OF THE F-8 DIGITAL FLY-BY-WIRE SYSTEM	October 1981
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
L.D. Brock and H.A. Goodman	R-1324

9. Performing Organization Name and Address	10. Work Unit No.
The Charles Stark Draper Laboratory, Inc. 555 Technology Square Cambridge, Massachusetts 02139	11. Contract or Grant No. NAS4-2571
	13. Type of Report and Period Covered Contractor Report
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration Washington, D.C. 20546	14. Sponsoring Agency Code RTOP 512-54-14

15. Supplementary Notes

NASA Technical Monitor: Kenneth J. Szalai, Dryden Flight Research Center

16. Abstract

The NASA F-8 Digital Fly-by-Wire (DFBW) flight-test program is intended to provide the technology for advanced control systems, giving future aircraft enhanced performance and operational capability. A detailed analysis of the experimental system was performed to estimate the probabilities of two significant safety-critical events: (1) loss of primary digital flight-control function, causing reversion to the analog bypass system; and (2) loss of the aircraft due to failure of the electronic flight-control system.

The analysis covers appraisal of risks due to random equipment failures, generic faults in design of the system or its software, and induced failures due to external events. A unique diagrammatic technique was developed which details the combinatorial reliability equations for the entire system, promotes understanding of system failure characteristics, and identifies the most likely failure modes. The technique provides a systematic method of applying basic probability equations and is augmented by a computer program written in a modular fashion that duplicates the structure of these equations.

Results of the analysis indicate that the F-8 DFBW system has a very high reliability when used in typical 1-hour experimental flights, and no single failure can cause a system failure. However, the analysis shows a rapid increase in failure rate as a function of mission time. Therefore, basic design changes would be needed for commercial applications to either increase levels of redundancy or to provide reconfiguration capability to replace failed elements and maintain a more constant failure rate.

17. Key Words Suggested by Author	18. Distribution Statement
Reliability analysis Fly-by-wire Electronic flight control	Unclassified-Unlimited STAR Category 08

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price*
Unclassified	Unclassified	151	A08

*For sale by the National Technical Information Service, Springfield, VA 22161